The Report of the

2017 NSF Cybersecurity Summit for

Large Facilities and Cyberinfrastructure

Ensuring Data Provenance, Integrity and Resilience

August 15 - 17, 2017

Westin Arlington Gateway - Arlington, VA

https://trustedci.org/2017nsfsummit/

Acknowledgements

The organizers wish to thank all those who attended the summit. Special gratitude goes to all those who responded to the CFP, spoke, provided training, and actively participated, including the 2017 Program Committee (highlighted in Section 5), without whom the event would not have been as successful. Our sincere thanks goes to the National Science Foundation and Indiana University's Center for Applied Cybersecurity Research for making this community event possible.

This event was supported in part by the National Science Foundation under Grant Number 1547272. Any opinions, findings, and conclusions or recommendations expressed at the event or in this report are those of the authors and do not necessarily reflect the views of the National Science Foundation.

About this Report

This document is the product of Trusted CI: The NSF Cybersecurity Center of Excellence and was supported by the National Science Foundation under the grant - ACI-1547272.

Citing this Report

Please cite as: James Marsteller, Von Welch, Mark Krenz, Andrew Adams, Scott Russell. Report of the 2017 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities: *Ensuring Data Provenance, Integrity and Resilience*. http://hdl.handle.net/2022/21882

License

For the latest information on the Summit

Please see, https://trustedci.org/summit/

Table of Contents

Executive Summary

The 2017 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure (CI) continued to build a trusting, collaborative community working to address core cybersecurity challenges in support of NSF science. The 2017 summit built on the success, findings, and lessons learned from previous years, and focused on the theme of "*Ensuring Data Provenance, Integrity and Resilience*". The program committee and presentations submitted by community members drove the program. A call for participation (CFP) resulted in thirty seven (37) proposals consisting of: 15 plenary topics, and 11 training sessions, 6 student applications and 5 table talks. For the third year in the row, the summit received a marked increase in CFP proposals, again exceeding our capacity to accommodate them all.

The 2017 summit took place in Arlington, VA, August 15th through midday August 17th. On August 15th, it offered a full day of training. The second and third days consisted of plenary sessions designed to address the theme of "Ensuring Data Provenance, Integrity and Resilience" in the context of cyberinfrastructure projects and Large Facilities.

One hundred twenty three individuals attended the summit, with 48 individuals -- more than one third of all registrants -- participating in planning, speaking, providing training, co-authoring a CFP submission, and/or leading a lunch table talk. In all, 56 NSF-funded projects, including 18 Large Facilities, were represented. Attendee evaluations and feedback were overwhelmingly positive and constructive.

The 2017 summit continued to make progress on the recommendations and opportunities defined at the 2016 summit, identifying findings, recommendations, and future challenges for the NSF community. A full list of findings, recommendations, and future challenges is delineated in Section 4 of this report, but the following are the key recommendations derived from the 2017 summit:

Recommendation 1: NSF projects should have budgets for cybersecurity in the range of 3-12% of total IT budget. Projects with cybersecurity budgets below that range should carefully consider the appropriateness of their budget.

Recommendation 2: NSF projects should engage and incorporate stakeholders and senior leadership into the information security risk acceptance and risk management processes. This should include explicitly delineating responsibilities and accountability among the relevant actors.

Recommendation 3: NSF projects should look to a broader range of cybersecurity standards and frameworks when selecting what will provide the best fit for their mission.

Recommendation 4: NSF projects should continue to refine Risk-based approaches to help provide the most nuanced and applicable information to cybersecurity stakeholders, and may wish to draw from a broader range of sources, such as the AFCEA Economics of Cybersecurity and the Information Security Practice Principles.

Organizers' Thoughts

We continue to be extremely happy with the impact the summit is having in terms of bringing the community together, soliciting responses to the call for participation, and fostering sharing experiences amongst the community. We thank the community members who enable this success through their participation at the summit. In particular we thank those who serve on the program committee.

This year interest in the summit hit a record high, representing a 20% increase in attendance over 2016. We're excited to see a third year of growth in community participation and response to the call for proposals, again exceeding the program's capacity to accommodate. We do believe however that we, the program committee, and the community should not become complacent. With our established trust and sense of community, we should consider and continue to refine our ongoing and long-term goals to ensure we continue to produce new successes as well as adapt to changes in the cybersecurity and NSF landscapes. We will continue to evolve and adjust the summit in order to meet the community's changing needs.

Next year we'll follow the NSF office move and hold the summit to Alexandria, VA. We note that while community interest in the summit was the strongest in history, NSF participation hit a low with only nine employees attending. With declining participation from the NSF, the program committee may consider holding future summits in other locations that have been requested by the community. Additionally, with the increased growth of the summit, we plan on charging a registration fee in 2018 to offset the added costs.

Finally, we thank the program committee members for their hard work and devotion to the summit, and we thank NSF for funding the summits and providing presentations.

-2017 Summit Organizers: Leslee Cooper, Ryan Kiser, Mark Krenz, Jim Marsteller, Amy Starzynski Coddens, Diana Borecky, and Von Welch.

1 Background: Evolving Cybersecurity Landscape, and Advancing Trustworthy Science

CTSC, now in its sixth year, reestablished the annual NSF cybersecurity summit as a means to reinvigorate the NSF cybersecurity community and increase trust in the science supported by that community. The summit serves as a valuable tool for securing NSF scientific cyberinfrastructure (CI) and increasing trust in the science it supports by providing a forum for education, sharing experiences, and building community. For many attendees, the summits are unique opportunities to come together with their colleagues, to benchmark and debate cybersecurity best practices, and to receive practical, relevant training.

Although the summit offers value across the community, it is of particular value and importance to NSF-funded cybersecurity professionals, NSF Program Officers, and Trusted CI. The summit offers a forum for these diverse stakeholders to come together and share experiences, identify common challenges, and network. The summit also provides a venue for the development of an NSF cybersecurity community, increasing collaborations and connections between diverse institutions. Moreover, the summit presents an excellent opportunity to highlight cybersecurity challenges to program officers, leadership, and stakeholders, as well as provide basic cybersecurity awareness and educations functions. Finally, the summit presents an opportunity for Trusted CI to gather insight into the needs, concerns, and challenges facing the community.

The constantly changing state of cybersecurity is one that can be challenging for any organization, whether commercial, academic or governmental. Florence Hudson, Senior Vice President & Chief Innovation Officer of Internet 2, observed at the conclusion of the summit that some things in our environment haven't changed while others have and suggested further exploration. Rapidly changing technology (e.g., Internet of Things; Cloud Services) and ever-evolving and diverse threats present new challenges, while others, such as economic challenges and workforce readiness, have existed for some time.

Addressing these challenges is fundamental for supporting and advancing trustworthy science. During the summit opening, Director of the Office of Advanced Cyberinfrastructure (OAC) Irene Qualters highlighted the core principles of promoting science excellence and focusing on unique NSF contributions to CI, enabling fundamentally new scientific advances, and incorporating new approaches and technologies to support these OAC principals.

Ms. Qualters also shared responses to the 2030 strategy development process request for information (RFI) that will impact the future landscape of cyberinfrastructure. The responses seek a vision of the future with an integrative ecosystem, built on robust, secure, and dynamic

workflows and data flows across diverse technologies and boundaries. This ecosystem would include multi-institutional authentication for distributed communities and at-scale security approaches for research communities. Other themes included trustworthy software and data for robust and reliable science, emphasis on both human and technical capabilities, and finally, commitment to continuity of CI and links to research. The results from the survey show the need for ongoing integration of new technologies and increasing collaborative frameworks, all of which must be evaluated and implemented in a secure fashion to advance trustworthy science.

The 2017 summit took place Tuesday, August 15th through midday Thursday, August 17th, at the Westin Arlington Gateway near NSF. On August 15th, the summit offered a full day of training that included a record-high six parallel sessions. The second and third days followed a workshop format designed to identify both the key cybersecurity challenges facing Large Facilities and the most effective responses to those challenges. The event brought together leaders in NSF CI and cybersecurity communities to continue the processes initiated in 2013: building a trusting, collaborative community, and seriously addressing that community's core cybersecurity challenges.

The remainder of this report is structured as follows: Section 2 outlines the summit's purpose, scope, and theme; Section 3 provides summaries of the presentations; Section 4 identifies the Findings, Recommendations, and Future Challenges identified from the Summit; Section 5 lists the organizanizing and program committee; Section 6 replicates the CFP and summit program; Section 7 provides details on the summit's attendance and participation; Section 8 provides the results of attendees' evaluations of the event, and Section 9 catalogues lessons learned. The report concludes with the closing thoughts of the organizers.

2 The Summit's Purpose, Scope, and Theme

The theme of ***"Ensuring Data Provenance, Integrity and Resilience"*** was selected by the program committee for the 2017 summit. The theme was introduced during the first keynote, "A Workflow-Centric Approach to Increasing Reproducibility and Data Integrity" (see Section 3), where Jeff Spies delved into the moral and ethical impact scholarly values had on data integrity. Marjory Blumenthal's keynote, "Data, data, everywhere—how shall we live with it?", reinforced the theme directing the audience's attention to big data and the need for privacy based on provenance. Not only did Marjory point out that the subject (the data user) rarely has a relationship with the data collector, but she expanded on the summit's theme by suggesting a new attribute or metric, veracity, which could be used to reflect the accuracy of the data.

Similarly, two panels, “Cybersecurity in the Face of Overwhelming Threats and Cloud Security” and “NSF Partnerships with Cloud Providers” further pushed the scope of the summit beyond the need to understand how provenance, integrity and resilience affect data to additionally exploring and sharing mechanisms to ensure its security. The first discussed measures and techniques science projects should undertake to secure data in the face of adversaries, while the latter presented approaches major Cloud service providers currently implement to ensure data security.

The 2017 summit built on the recommendations of past summit reports,[1] which we’ve documented in section 4 of this report ***“Progress Towards Priority Recommendations”.***

We believe the summits are critical in supporting measurable progress on the following goals: identifying, establishing and sharing community standards for best practices regarding cybersecurity; providing pragmatic levels of information security; meaningfully addressing software assurance, quality or supply chains in the context of the project cybersecurity programs; and supporting scientific discovery.

3 Summit Program Summaries

A Workflow-Centric Approach to Increasing Reproducibility and Data Integrity - Jeff Spies delivered the first keynote. His presentation discussed the need for increased research efficiency, quality, inclusivity, and diversity, by highlighting that a gap exists between scholarly values and practices. Specifically, that peer review introduces bias. To combat this, he argued that the science community needs to focus more on replicability, that is, holding methods constant than to reproducibility that attempts to hold data constant. Moreover, his findings showed that the lack of replicability is tied to the desire and need for scientist to get their research published. Jeff concluded by questioning whether or not we can address the incentives for science by moving peer review to immediately after the theory governing the research, but before the data generation process in order to remove bias in the latter phase.

From Bare Metal to Virtual: Lessons Learned when a Supercomputing Institute Deploys Its First Cloud - Evan F. Bollig presented on their experiences at the Minnesota Supercomputing Institute (MSI). His talk not only described the lessons learned when the MSI launched it’s first cloud-based platform to support research with specific data use agreements, but it also addressed issues concerning accountability, risk acceptance, and the role of project leadership

[1] See the 2015 summit report, agenda, and more at http://trustedci.org/2015summit/

when a large supercomputing facility deviates from its traditional base of support.

Key issues from his talk centered on their virtualization software not being able to satisfy four core needs: on-demand resources, long-running jobs, container-based computing, and NIH Controlled data (dbGaP) ¾ petabyte of data. Similarly, Minnesota's OIT was not prepared to handle controlled data. These challenges forced MSI to re-evaluate requirements and planning.

Cornell Red Cloud: Campus-based Hybrid Cloud Computing - Steven Lee relayed concerns around securing hybrid cloud systems for research, while focusing on lessons learned from architecting and implementing Cornell's Red Cloud service, a Eucalyptus-based cloud system which provides a set of virtual machine systems for users with non-traditional computational needs that is API-compatible with Amazon services. The session covered some of the practical cybersecurity concerns with running a hybrid cloud system.

Cybersecurity in the Face of Overwhelming Threats - Von Welch, moderator, and panelists, Michael Corn (UCSD), Anita Nikolich (NSF), and Kim Milford (REN-ISAC) discussed in the first panel what a science project should do in the face of being targeted by an adversary with significant (more than the project has) resources, who is very motivated and has access to significant "cyber weapons" (vulnerabilities, malware, social engineering techniques). Similarly, what should the community do if one of those threat's persistent attention was to be turned on to a project in the NSF community?

The panelist addressed these questions by first emploring that research projects make certain that they have sufficient methods in place, e.g., backups, incident response, to ensure the survival of the data A secondary recommendation was stronger NSF requirements for securing NSF projects.

HTCondor - Todd Tannenbaum delivered a "lessons learned" type talk about the security-related challenges HTCondor has faced and the resulting mistakes, solutions, and policies developed during the past 20 years of creating and distributing HTCondor. Topics included what security-related policies and procedures that every production software project should have in place, and an overview of some of the time-tested processes evolved within the HTCondor team on vulnerability response, personnel organization, and defensive coding. Topics were presented first as a description of the problem to be addressed, and while some of the material was aimed at software engineers, most of the presentation was at a level easily approachable by non-developers such as project managers and principle investigators without a computer science background.

A lost maxim that was conveyed, was that security hygiene is not just for projects that use the internet, run as root, or have sensitive data, for tools that appear to have banal security

requirements can be leveraged as agents to compromise and escalate permissions within a system. Moreover, Todd espoused on the challenges in communicating and mitigating vulnerabilities within an open-source environment, without furthering the possibilities of attacks due to its public nature.

Strategies to Develop a Diverse and Inclusive Cybersecurity Pipeline - moderator Tony Baylis, along with panelists, Aurelia Williams (Norfolk State University), Victor Piotrowski (NSF), Rodney Petersen (NIST), and Ambareen Siraj (Tennessee Tech University/WiCyS) explored efforts and initiatives employed to grow, recruit, and educate a diverse and inclusive pipeline of cybersecurity professionals for our workforce needs. For without the full participation of a diverse workforce, the economic viability of the nation is threatened and the creativity to shape future technology is lost.

The panelist conveyed that several programs, specifically in training cybersecurity specialists, are instantiated in both the NSF and NIST. Additionally, WICSY (Women in Cybersecurity) and some college and university curriculums are available to encourage minorities to pursue an education in cybersecurity. Questions that were presented to the panelist focused on awareness to potential students and tapping into the resources developed by the programs.

Beyond the Beltway: The Problems with NIST's Approaches to Cybersecurity and Alternatives for NSF Science - Craig Jackson, Bob Cowles, and Scott Russell spoke about and examined the differences between RMF, SP 800-171, and CSF, and postulated that they are inefficient and ineffective approaches to cybersecurity and cyber resilience. To support this, they offered perspectives from the DoE, defense and legal communities. Moreover, they showed that NIST's products are ill-suited to the resources of NSF science projects. Finally, the speakers commented on alternate choices that could be adopted, including, CIS's Critical Security Controls and the Australian government's Essential Eight.

Finding Your Way in the Dark: Security from First Principles - Susan Suns introduced a mental model for reasoning about security instead of trying to memorize for security and demonstrate its application to real-world examples. Her goal was for attendees to leave looking at the technologies and human systems around them a little differently.

Susan's main focus was the idea of using principles, including: comprehensivity, opportunity, rigor, minimization, compartmentation, fault tolerance, and proportionality, to teach people to "*think like a security practitioner*".

Data, data, everywhere—how shall we live with it? - Marjory Blumenthal gave the second keynote. Her talk centered on big data and its need for privacy. It was postulated that privacy policy within the US is legislated on "small data", where the subject has a relationship with the

data collector. However, with ease of storing and collecting big data, the relationship could be nonexistent. This is especially prevalent to online education, health care, and smart homes, where it is unclear how the collected data is being used, or by whom.

Marjory additionally introduced a new attribute to the canonical CIA (confidentiality, integrity and availability), referred to as veracity that reflects the accuracy of the data. She closed the discussion stating possible directions for solutions, suggesting both better tools to support anonymization and encryption, as well as stronger legislature.

Cloud Security & NSF Partnerships with Cloud Providers - moderator Susan Ramsey, panelists Susie Adams (Azure/Microsoft), Mark Ryland (AWS), and Matthew O'Connor (Google) participated in the last panel of the Summit. The panel provided an opportunity for Cloud vendors to discuss their approach in handling data integrity within the Cloud. The importance of this discussion is justified by the increasing requirement of universities to comply with NIST 800-171 CUI, or FISMA, along with other stipulations or costs that are driving the universities to use Cloud solutions.

One revelation that came from this panel was that all three service providers incorporated differing levels of accreditation to FISMA, FedRAMP and 800-171, although the reasons behind the varying levels was less clear. However, having a mechanism to provide feedback to NIST was suggested as a possible solution. Moreover, it was reasoned that FISMA and FEDRAMP are controls-based, where as the Cloud providers base much of their security on anomaly detection in an effort to protect data where it lives.

The Applicability of HPC for Cyber Situational Awareness - Leslie Leonard discussed the High Performance Computing Modernization Program (HPCMP), a central resource for expertise in the application of high-end computing to the Department of Defense's most challenging problems. She spoke on their high-level goals, research challenges, and anticipated results for cyber SA using the HPC Architecture for Cyber Situational Awareness (HACSAW), which is a HPCMP developed initiative to leverage HPC to advance emerging challenges for Cyber Situational Awareness (SA). She showed how HACSAW can provide a computational and data rich environment to researchers and collaborators to test, develop, model, measure and refine data-driven analytics. Additionally, that his environment will be the proving ground for novel ideas, algorithms and approaches that are suitable for large scale execution with dedicated HPC.

Internet2 NOC Risk Assessment - Paul Howell provided a baseline security risk assessment of the Internet2 network and Network Operations Center (NOC) that identified specific improvements designed to better protect the network and the services dependent upon the IT from attacks. He related on several critical improvements that improved the network's

resistance to attack, and further showed how these efforts could yield a sustainable security program that would enable Internet2 to appropriately manage the risks from increasingly sophisticated and targeted attacks and promote a culture of security.

4 Progress Towards Priority Recommendations

The 2017 Summit continued to make progress on Recommendations and Opportunities set out in past summits, while also introducing new important themes and issues to the community.

The remainder of this section is broken into three parts: Section 4.1, "Findings," will lay out factual information collected from the current year's summit; Section 4.2, "Recommendations," will offer specific guidance to the community based on this year's Findings and past years' Findings and Recommendations; and Section 4.3 "Future Challenges," will suggest important work that still needs to be done in the community and offer potential themes and topics for future summits.

4.1 Findings

Findings are factual determinations made as a result of the Summit. Findings serve to provide insight into the cybersecurity landscape of the NSF Community, and help form the basis for Recommendations and Future Challenges.

4.1.1 Risk Management:

The 2017 Summit came away with a number of findings regarding the adoption and implementation of risk management processes. There was widespread agreement that incorporating stakeholders and leadership into the risk management process is important for NSF science facilities. Similarly, there appeared to be consensus that more explicit incorporation of proportionality and mission concerns into risk management was valuable for building stakeholder support. Finally, several participants voiced a need to more explicitly prioritize risks given their limited resources.

However, there was still some disagreement regarding risk management frameworks, particularly regarding the efficiency and effectiveness of NIST approaches, with numerous speakers and panelists voicing criticisms of the NIST approaches, while others proved more supportive of these standards.

4.1.2 Baseline Security:

A second area of findings related to establishing a baseline set of controls for security programs. Specific controls that were suggested included two-factor authentication, periodic

risk assessments, and restricting privileged access/implementing least privilege. However, several other controls frequently were discussed, including audits (viewed by some as more valuable than outright prevention controls), bug bounty programs, and placing a greater emphasis on system architecture rather than focusing on code.

4.1.3 Regulation:

The spectre of regulation was a third area of findings. Controlled data (PHI, CUI, PII, etc.) was a particular concern, and most institutions who are already managing controlled data identify it is a source of problems. In addition, a recurring sentiment was that most regulations have not kept pace with technological changes, and prove inflexible for those who must adhere to them. Several institutions voiced interest in building partnerships or in outsourcing cybersecurity functions completely (e.g. through cloud providers) as a means to avoid dealing with regulations directly.

4.1.4 Summit Impact:

Finally, there was considerable agreement regarding the value the Summit and its related cybersecurity materials provide to the community. The Large Facility Manual security section was touted as valuable resource, with its primary shortcoming being its lack of visibility for the broader community. Similarly, summit trainings were extremely popular, and prompted several comments about increasing the number of and access to trainings. Suggestions included more in person training during the summit, online access to summit trainings, and additional online training offered throughout the year. Finally, the Summit more broadly had a direct impact on most attendees, with a clear majority identifying themselves as having at least one action item in response to the Summit.

4.2 Recommendations

Based on the findings of this year's summit and the accumulated findings and recommendations from past years' summits, (listed in Appendix A), we have come to the following recommendations for the NSF science community. Recommendations are intended to offer specific guidance to the broader NSF community, and should serve as a foundation for recommendations for future summits.

4.2.1 Budgets

The importance of information security budgets has been a recurrent topic within the NSF community. The issue of budgets was raised at the 2015, 2016, and 2017 summits, including a specific presentation by Jackson, Cowles, and Russell in 2016. Furthermore, the 2015 and 2016 Reports both list as Recommendation 1 that "The NSF CI and Large Facility community should

develop a broadly applicable strategy for information security budgets, including how, why, and where it does what it does in terms of spending." Less formally, a number of presentations and discussions included conversations of budgets.

Based on this recurring importance, and the compiled findings of three years of summits, we reach our first recommendation:

> **Recommendation 1:** NSF projects should have budgets for cybersecurity in the range of 3-12% of total IT budget. Projects with cybersecurity budgets below that range should carefully consider the appropriateness of their budget.

4.2.2 Risk Management

Understanding and applying risk management concepts has been a recurrent concern for the NSF science community. Questions related to appropriate and effective risk management have been raised at the previous four summits, with Recommendation 2 (2014), Recommendation 4 (2014), Recommendation 3 (2015, 2016), Recommendation 5 (2015, 2016), and Recommendation 6 (2015, 2016) all relating to risk management. Furthermore, a number of presentations and comments have spoken either directly or indirectly on the need to better understand and engage in risk management practices.

Based on this recurring importance, we reach our second recommendation:

> **Recommendation 2:** NSF projects should engage and incorporate stakeholders and senior leadership into the information security risk acceptance and risk management processes. This should include explicitly delineating responsibilities and accountability among the relevant actors.

4.2.3 Risk Management Resources

The community's interest and engagement with risk management topics has also led to considerable interest in specific risk management frameworks to help structure risk-based decision making. The issue of whether and what specific frameworks to adopt, their strengths and limitations, and anecdotal experiences implementing them has been a popular topic for discussion. Recommendation 5 (2015, 2016) highlighted the need for the community to adopt a broadly applicable framework, and specific presentations in 2015, 2016, and 2017 all addressed the potential benefits and drawbacks of specific frameworks offered by NIST, such as the Risk Management Framework, Cybersecurity Framework, and Special Publication 800-53.

Based on this ongoing and unsettled discussion, we selected our third recommendation:

> **Recommendation 3:** NSF projects should look to a broader range of cybersecurity

standards and frameworks when selecting what will provide the best fit for their mission.

Furthermore, numerous presentations highlighted potential cybersecurity resources, with the CIS Critical Security Controls, Australian Signals Directorate Essential 8, Information Security Practice Principles, and AFCEA Economics of Cybersecurity all offering unique and useful cybersecurity perspectives. While these sources are not intended to be definitive or exhaustive, they offer value to the community and should be considered when engaged in risk management processes.

Based on this growing body of sources, we reach our fourth recommendation:

> **Recommendation 4:** NSF projects should continue to refine Risk-based approaches to help provide the most nuanced and applicable information to cybersecurity stakeholders, and may wish to draw from a broader range of sources, such as the AFCEA Economics of Cybersecurity and the Information Security Practice Principles.

4.3 Future Challenges

Additionally, we would like to highlight areas of current concern, note, or interest that we believe should serve as springboards for future discussions and collaborations in the broader community. Future Challenges are intended to be more open ended, and should prompt discussion and consideration in the broader community. Although we expect these "Future Challenges" to serve as part of our calculus when accepting CFPs in future summits, they will still only be one factor in a multi-factor test.

> **Challenge 1:** (Cloud Computing Information Sharing)The NSF CI and Large Facility community should explore ways to more effectively share information regarding cloud computing platforms. This should include information about the use of third party providers, and about running your own cloud systems.
>
> **Challenge 2:** (Collaboration) The NSF CI and Large Facility community should find more ongoing ways of collaboratively developing and maintaining cybersecurity programs, such as sharing materials, services, practices, lessons learned, and collaborative/peer reviews.
>
> **Challenge 3:** (Identity Management) The NSF CI and Large Facility community should continue to develop and disseminate best practices for identity and access management to support research.
>
> **Challenge 4: (**Artificial Intelligence) The NSF CI and Large Facility community should

explore the role that Artificial Intelligence, Machine Learning, and other advances in automation may play in the future.

Challenge 5: (Privacy) The NSF CI and Large Facility community should continue to determine the impact of privacy on their projects. New data protection regulations such as the General Data Protection Regulation (GDPR) may affect projects collecting data on European people.

Challenge 6: (SWA) The NSF CI and Large Facility community should determine its software assurance, quality, and supply chain requirements, and determine whether their goals regarding software security may yield some unmet requirements in this space.

5 The Organizing and Program Committees

The 2017 summit was organized and hosted by the NSF Cybersecurity Center of Excellence, and six members of that project (Ryan Kiser, Jim Marsteller, Mark Krenz, Amy Starzynski Coddens, Diana Borecky and Von Welch) along with Leslee Cooper, the Administrative Director for the IU Center for Applied Cybersecurity Research, served as the organizing committee. We recruited a Program Committee (PC) made up of key leaders from NSF CI projects and the broader community. The PC was to be responsible for setting the agenda and inviting speakers, evaluating and selecting from among proposed training, talks and panels, extending invitations to expert presenters, participating actively in the event itself, and laying the framework for successful post-summit evaluation and community support. Jim Marsteller served as chair of the PC, a role he has held in prior summits. The PC held 14 meetings by conference call beginning March 13, 2017 and ending August 28, 2017. It conferred electronically both prior to and following this time period, with monthly meetings.

The 2017 PC members were:

- **Steve Barnet,** Senior System Administrator for the IceCube Neutrino Observatory.
- **Anthony (Tony) Baylis**, Assistant Department Manager for the Computing Applications and Research Department in the Computation Directorate at Lawrence Livermore National Laboratory.
- **Michael Corn**, CISO of the University of California at San Diego where he manages the Security Office as well as the Identity and Access Management..
- **Rion Dooley,** Principal investigator on the Agave Project a Science-as-a-Service API

platform allowing researchers worldwide to manage data, run code, collaborate freely, and integrate their science anywhere.

- **Barbara Fossum**, NEES deputy center director and former managing director of Purdue University's Cyber Center and Computer Research Institute.
- **Dr. David Halstead**, CIO for the National Radio Astronomy Observatory. His responsibilities are divided between Data Management for the Observatory's HPC infrastructure in support of the national radio telescopes, and the general IT support for NRAO's 500+ employees.
- **Ardoth Hassler**, Associate Vice President of University Information Services & Executive Director, Office of Assessment and Decision Support at Georgetown University and former Senior Information Technology Advisor in the Office of the Chief Information Officer in the NSF Office of Information and Resource Management, Division of Information Systems.
- **Susan Ramsey**, Risk Assessor and Security Engineer at the National Center for Atmospheric Research.
- **George Strawn**, NAS as board director for the Board on Research Data and Information, Formerly NSFnet program director and then division director of networking), then CISE executive officer and acting assistant director, and then served as CIO. He was detailed to OSTP in 2009 where he served as director of the NITRD NCO.

6 The Call for Participation and Program

The full agenda and biographies are attached to this report as Appendices A and B[2].

The PC issued a call for participation (CFP) to the community requesting submissions in the form of: (a) white papers one to five pages in length, focused on unmet cybersecurity challenges, lessons learned, and/or significant successes, (b) one to two-page abstracts for proposed half and full-day trainings, (c) one to two page abstracts for proposed table talk sessions, or (d) student applications.[3] Additionally, the PC invited specific community leaders as

[2] The full summit program is also available on the CTSC website, https://static1.squarespace.com/static/5047a5a6e4b0dcecada15549/t/598e0aa03e00bedb674b6381/1502481057079/Program+Agenda+-+2017+NSF+Summit.pdf

[3] https://trustedci.org/2017-nsf-cfp/; see also Appendix C.

well as experts from outside the community to give presentations and participate in panels.

The CFP continued a process started in 2014, designed to elicit a greater degree of community participation in developing the agenda, executing the summit, and increasing our ability to identify summit findings that represent the concerns, successes, and aspirations of our community. The 2014 CFP process was expanded in 2015, and a "Tips for Building CFP Responses" was provided to guide and encourage respondents and additional content formats were considered. The 2017 CFP process proved a success, and drove a great deal of the resultant program, including a mix of 15 plenary submissions, 5 table talks, 11 training sessions, including a full day workshop as well as a keynotes from the community at large, and presentations from key leaders from within the NSF community. For the third year in the row, we received a marked increase in CPF proposals, again exceeding our capacity to accommodate.

The Summit program spanned two and a half days from August 15 through 17. On August 15th, we offered a full day of training. Descriptions of each training session are appended as Appendix D.[4] On August 17th and 18th, the Summit followed a plenary format with talks invited by the program committee and accepted from the CFP responses. Dr. Irene Qualters, Division Director of NSF/OAC welcomed the attendees and Jeff Spies, co-founder and Chief Technology Officer of the Center for Open Science (COS) gave an invited keynote. The program of submitted talks then commenced with talks on the NSF Cybersecurity Center of Excellence, and lessons learned at Minnesota Supercomputing Institute, Cornell, HTCondor. Two panel talks covering the topics of Cybersecurity threats and diversity and inclusiveness in the Cybersecurity workforce were also presented. The first day then concluded with talks on the topic of alternatives to NIST's and security first principles.

Day two opened with an invited keynote from Marjory Blumenthal, senior policy analyst and director of RAND's Science, Technology, and Policy Program. Her keynote discussed the impact of big data & privacy. Presentations then continued with a panel on cloud security supported by representatives from some of the biggest in the market today and a sharing the lessons learned of the Internet 2 NOC risk assessment.

7 Participants

This year registration was open to all interested individuals, a change we first made in 2016. This was done to avoid being insular, maintain and develop new relationships, and encourage

[4] See also, https://trustedci.org/2017training/

infusion of additional perspectives. Registration was granted to all parties who requested attend and were able to demonstrate a connection to the community. As with prior summits, registration was free, and, as in previous years, invitations were sent to a predetermined list of individuals. Our invitation list was based on the invitation list from the 2016 summit, and was updated to account for changes in the community, suggestions from NSF staff, and speakers to address specific topics of the summit. The invitation list included those with direct cybersecurity responsibilities in NSF Large Facilities and CI projects, NSF project principal investigators, and other key stakeholders and risk owners to ensure that NSF cybersecurity evolves to address their needs. Interest in the 2016 summit was so strong we hit our registration limit much earlier than any previous year.

Fig. 1 NSF Summit Attendees

One hundred forty seven (147) individuals requested registration for the summit, 141 registered, and record 123 attended (including speakers, tutorial presenters, panelists, students and the program committee). A listing of the attendees and their affiliations is in Appendix E. Eighty three attendees participated in the August 15 training sessions. Forty five individuals - over a third of participants - participated in planning, spoke, provided training, co-authored a CFP submission, and/or led a lunch table talk. Six attendees were students. Twenty nine attendees work at Large Facilities. Nine attendees work at the NSF.

This year we were excited to welcome WISE who held full day workshop at the summit[5]. WISE includes representative from many European E-Infrastructures including SURF, Hikhef, GÉANT, EGI, CERN, PRACE and EUDAT. The workshop featured US and International security experts collaborating on a variety of topics including the pDNS Data Sharing project, the impact of IoT devices on security, SoftWare Assurance and Risk Management.

[5] https://wise-community.org/2017/08/16/wise-feedback-gathered-at-the-nsf-summit/

7.1 NSF Project Representation

Attendees were asked to provide the NSF project or other organization (NSF directorate in the case of NSF staff) with which they were associated including the NSF award number if applicable and their NSF Directorate. The following list contains a normalization of the provided answers. We count 57 projects including 18 large facilities(marked with "♦"), were represented at the summit by representatives of those projects. Additionally, eight more Large Facilities were represented by NSF program officers (marked with "♦*"). NSF directorates represented by program officers only are marked with "*". NSF directorates represented in some manner include: OAC, GEO/OCE, CSE/CNS, MPS/APS, MPS/PHY, MPS/AST, MPS/DMR , ENG/CMMI, EHR/DGE, GEO/ICER, GEO/EAR and CCF.

We note some answers given represent NSF projects (e.g. "CC*IIE") or other general areas of the NSF community (e.g. "Science Gateways") which are not very precise and we will work on obtaining more precise specification of awards in future summits to improve our understanding of community representation.

- Academic Research Fleet (ARF) ♦*
- The Agave Platform: An Open Science-As-A-Service Cloud Platform for Reproducible Science
- A Single-Site I/UCRC Center for Research in Storage Systems (CRSS)
- Northeast Tier 2 Center (NET2) (Part of ATLAS)
- Atacama Large Millimeter Array (ALMA) ♦
- Blue Waters
- CC*DNI DIBBs: Data Analysis and Management Building Blocks for Multi-Campus Cyberinfrastructure through Cloud Federation *
- Center for Trustworthy Scientific Cyberinfrastructure (CTSC) *
- CC-NIE Integration: Leveraging DYNES for Weather Data Distribution on Multicast Virtual Circuits (NSF #1340910)
- Collaborative Research: CICI: Regional: SouthEast SciEntific Cybersecurity for University Research (SouthEast SECURE) *
- CICI: Data Provenance: Collaborative Research: Provenance Assurance Using Currency Primitives *
- Collaborative Research: CICI: Secure and Resilient Architecture: Data Integrity Assurance and Privacy Protection Solutions for Secure Interoperability of Cloud Resources *
- Compact Muon Solenoid (CMS) detector at CERN ♦*
- CyberCorps: Scholarship for Service Advanced Technological Centers Secure and

Trustworthy Computing

- DataONE (Data Observation Network for Earth) *
- Daniel K. Inouye Solar Telescope (DKIST)
- Developing a Software Artifact Repository for Software Assurance Education **(**NSF #1522847) *
- EAGER:Cybermanufacturing:Collaborative Research: A novel process data analytics framework for IoT-enabled cybermanufacturing
- EarthCube *
- Enabling Cybersecurity Research Transition To Practice Acceleration *
- Extreme Science and Engineering Discovery Environment (XSEDE)
- Gateways to Discovery: Cyberinfrastructure for the Long Tail of Science
- GEMINI observatory ♦
- HTCondor *
- IceCube ♦
- International Ocean Discovery Program (IODP) ♦*
- iPlant Collaborative
- Japan-US Network Opportunity (JUNO)
- Laser Interferometer Gravitational-Wave Observatory (LIGO) ♦
- Large Synoptic Survey Telescope (LSST) ♦*
- MIR-Advanced Modular Incoherent Scatter Radar (AMISR)
- National High Magnetic Field Laboratory (NHMFL) ♦
- National Optical Astronomy Observatory (NOAO) ♦
- National Optical Astronomy Observatory (CTIO)
- National Radio Astronomy Observatory (NRAO) ♦
- National Solar Observatory (NSO) ♦
- National Center for Atmospheric Research (NCAR) ♦
- National Institutes of Health
- Natural Hazards Engineering Research Infrastructure (NHERI) ♦
- North East Storage Exchange (NESE) projectnese.org *
- NSF SFS Project (PI): Tennessee Cybercorps: A Hybrid Program In Cybersecurity *
- SF SFS Project (Lead PI): CyberWorkshops: Resources and Strategies for Teaching Cybersecurity in Computer Science (CReST) *
- NSF SFS Project (Lead PI): Capacity Building in Cybersecurity: Broadening Participation of Women In Cybersecurity through Women in Cybersecurity Conference & Professional Development *
- NSF TUES Type-I Project (PI): SecKnitKit (Security Knitting Kit): Integrating Security into Traditional Computer Science Courses *
- Ocean Observatories Initiative (OOI) ♦ *

- Open Science Grid (OSG)
- Regional Class Research Vessel Program ♦
- Science Gateways Community Institute
- Secure and Trustworthy Cyberspace *
- Seismological Facilities for the Advancement of Geoscience and EarthScope (SAGE)
- SHF: Small: Collaborative Research: Coupling Computation and Communication in FPGA-Enhanced Clouds and Clusters;
- SHF: Medium: Collaborative Research: Next-Generation Message Passing for Parallel Programming: Resiliency, Time-to-Solution, Performance-Portability, Scalability, and QoS
- SI2-SSE AttackTagger
- US-Ignite
- Very Large Array (VLA) ♦
- Wall of Wind (Florida International University) ♦
- WISE

Participation from NSF program officers at the Cybersecurity Summit continued to drop lower this year with 9 NSF staff attending. This is down from 12 in 2016 and 18 in 2015. The NSF was in the process of moving from Arlington to Alexandria in the weeks before and after the summit. We realize this move likely had a negative impact attendance.

7.2 Student Representation

In addition to professionals, the Summit supported the participation of six students. Students were encouraged to self-nominate to the program, but were also able to be nominated by a mentor or teacher. In order to be further considered, they were then asked to provide a one-page, 800-word maximum letter describing the student's interest in and any relevant experience with cybersecurity, emphasizing the benefit to the student and/or community of the student's attendance at the Cybersecurity Summit.

Fig 2. Students from 2017 NSF Cybersecurity Summit

The Program Committee reviewed all submissions with an interest in advancing diversity and inclusiveness, settling on the following exceptional six students:

Dominique Dalanni – (George Washington University), William Drake (Indiana University Bloomington), Nikita Golubets (Eastern Michigan), Sinjoni Mukhopadhyay (University of California, Santa Cruz, Imani Palmer (University of Illinois at Urbana-Champaign), Rachael Shima (California State Polytechnic University).

The selected student applicants were paired with mentors from the program committee and community to encourage their continued participation in cybersecurity and NSF cyberinfrastructure. Students and mentors were given one another's contact information prior to the summit and encouraged, but not required, to contact one another. However, each pair did communicate prior to the summit, allowing them to familiarize themselves with one another prior to meeting in person. Once at the summit, students and mentors met each day for breakfast and lunch, along with one night for the program committee dinner. These meet-ups allowed the students to ask any questions they may have and assist in networking, while allowing mentors to introduce and share the community with potential new members.

This program has shown success, and we have received positive feedback from both students and mentors.

7.3 Inclusiveness

Finding 4 from the 2013 summit stated "Future program committees should take on gender, age, and racial/ethnic diversity in the community and summit attendance as a strategic imperative for future summits." The organizers recognize that diverse participation is both a socially relevant outcome for NSF[6] and a particular challenge in the cybersecurity community in general[7]. Thus, in 2014, we expressly addressed the topic with the PC, identifying two members to spearhead efforts (Baylis, Hassler), and the group sought to encourage diverse participation via the invitees, speakers, panelists, and PC itself. Additionally, the CFP expressly gave priority to those students from groups underrepresented in the NSF information security workforce. We note that Baylis has specific experience in this area as chair of the Supercomputing Broader Engagement in 2008 and participated in that committee in 2009. Baylis and Hassler again spearheaded these efforts in 2017, building on the success seen in 2014, 2015 and 2016.

In order to gather ongoing baseline data related to this diversity effort, 2017 registrants had the

[6] *See*, NSF GPG, Section II.C.2.d.i

[7] *See, e.g.*, *Agents of Change: Women in the Information Security Profession.* A whitepaper derived from the 2013 (ISC)2 Global Information Security Workforce Study. Available from: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf

option to provide their ethnicity/race and gender/sex. There was a 4% increase in the number of female registrants in 2017, and only slight changes in the ethnicity/race of registrants, with an increase in diverse participants. The aggregated responses to the those items follow. Voluntary responses to these questions show:

Table 1. Attendee self-reported ethnicity.

Ethnicity / Race	
Asian or Southeast Asian	11 (8.4%)
Black or African American	4 (3.1%)
Hispanic or Latino	4 (3.1%)
Native Alaskan or American Indian	1 (0.8%)
Multiracial	4 (3.1%)
White or Caucasian	79 (60.8%)
Other Ethnicity	0 (0%)
Other (space provided)	1 (0.8%)
Prefer not to answer	10 (7.7%)
No Answer Provided	16 (12.3%)

Table 2. Attendee self-reported gender.

Gender / Sex	
Female	27 (20.8%)
Male	77 (59.2%)
No Answer Provided	26 (20.0%)

8 Attendee Evaluations

We sought attendee evaluations of the summit via two SurveyMonkey surveys. One survey gathered feedback on the summit generally; the other requested feedback specific to the August 15 training sessions. A summary of the general and training survey results are appended to this report as Appendix H.

8.1 Attendee Survey

The responses were generally very positive and extremely thoughtful. Forty-five attendees (approximately 37% of all attendees) responded to the general "Attendee Survey." The organizers did not submit responses, but the survey was open to all other participants. We did

not request the names of respondents, and have redacted some information from the appended report to further protect the anonymity of respondents.

The quantified and categorical results (e.g., rating scales, yes/no questions) were very favorable. Selections follow:

- To Question #5, "How would you rate your overall experience with the 2017 summit?" 33% of respondents selected "Good", while the remaining 66% responded with "Excellent."

- Regarding Question #7, "Was this summit better than what you expected, worse than what you expected, or about what you expected?" the summit at least met the expectations of everyone that responded, while exceeding the expectations of 86% of respondents.

- To Question #8, "How useful to your work was the information discussed at the summit?" 100% of respondents gave ratings of "moderately useful," "very useful," or "extremely useful," with 86% providing the higher two responses.

- To Question #9, "If you attended last year's summit, how does this year's compare?" 38% of respondents gave ratings of "this year's summit was about the same as last year's," "this year's summit was better than last year's," or "this year's summit was much better than last year's," with 28% providing the higher two responses. The remaining 62% of respondents indicated that they did not attend last year's summit.

- To Question #11, "Would you like to attend future summits?" 80% responded "Yes," while the other 20% responded "Maybe."

Questions 13 and 14 sought open-ended responses, and were designed to elicit critique and discern highly-valued aspects of the experience. While the generally positive results of the above-referenced questions provide context, these open-ended questions have proved a useful communication tool. Observations follow:

- Question 13 asked, "How can we improve the summit experience in the future?"

    - Of the 22 respondents to this question, 10 remarked on the training sessions, most suggesting that information from the training sessions should be further broadcast to reach extended audiences, e.g.:

        "As I've stated before that given the effort the instructors put into the training sessions, it would be very nice to record these and make them available for later viewing. At the federated management course I took

offered by Scott Koranda and Jim Basney, there were only a few people, and the quality of the course was very good and in the ideal world would be shared by a LOT more people... I suggest that starting "low-key" with recording the training sessions would work quite well - perhaps create a tradition of using students who now record notes at the lunch session reunions, to now also take charge of recording the training sessions. I think it is NOT NECESSARY at least at the beginning to buy a bunch of expensive equipment or hire specialists for this - it's amazing how good a quality you can get with a simple iPhone and a selfie stick - just check YouTube - some of the videos done this simply are amazingly good. Over time, it could become a tradition and I'll bet the high quality of the results will surprise."

- While 6 of the respondents commented on desires for future panels and talks. An example response follows:

  "Expand the training - perhaps 2 days? And bring back those guys from Microsoft, AWS and Google - that panel could have gone on for a couple more hours easily."

- Question 14 asked, "Were there any aspects of the summit you found particularly useful or important? If so, please explain."
  - Of the 21 respondents, 10 praised both the plenary discussions and talks that covered implementing security controls (e.g., FISMA, NIST 800-53), especially citing the input from the corporate representatives present. An example response follows:

    "The diversity panel and the "cloud" panel (Azure, Google and AWS) were outstanding. I urge you to continue to have at least one "privacy" session in the program. Loved the diversity of the speakers, both in the mix of "people" but also the topics and subjects."

8.2 Training Evaluation

The Training Day preceding this year's summit offered eight training sessions: 2 all day sessions, and 8 half day sessions. Each session was well attended, with topics and number of attendees as follows: WISC Workshop (14); Federated Identity Management for Research Organizations (8); Legacy Industrial Control System, Secure / Replace / Ignore? AM (4); Handling Regulated Government Data, Protected Health Information, and CUI AM (15); Security Log Analysis AM (15); Digital Forensics / Incident Response AM (6); Developing Cybersecurity Programs for NSF Projects PM (18); Shared Intelligence Platform for Protecting our National Cyberinfrastructure

PM (7); Rebuilding a Plane in Flight: Refactors Under Pressure PM (5); and Automated Assessment Tools - Theory & Practice PM (5). Each tutorial attendee was asked to fill out a tutorial-specific survey after each training session concluded.

The responses to the tutorial-specific surveys were very positive generally, and included constructive feedback, as well as ideas for future training offerings. For simplicity, we asked attendees to complete one survey with several repeated questions to allow sorting differentiated responses for morning and afternoon sessions. The aggregated ratings in Questions 1 through 10, and 13 through 18 are attached as Appendix H. We summarize a few aggregate responses below:

- To Question 3, “Based on your overall experience with the August 15 training sessions, would you participate in training offered at future summits?,” 10 of 11 respondents selected “Yes,” the last selected “Maybe.”
- To Questions 7 and 15, “How would you rate your overall experience with the [morning/afternoon] training?,” 90% of responses were “Excellent” or “Good.”
- To Questions 9 and 17, “Was this [morning/afternoon] training better than what you expected, worse than what you expected, or about what you expected?,” 100% of responses indicated that expectations were met or exceeded. Sixteen (76%) of responses were “Somewhat better,” “Quite a bit better” or “A great deal better.”
- To Questions 10 and 18, “How useful to your work was this [morning/afternoon] training?,” 71% of the responses (15 of 21) were “Very Useful” or “Extremely Useful.”

The responses for the individual tutorials were reported back to their respective tutorial leaders, including responses to Questions 11 and 19, “How can we improve this training session in the future?” and Questions 12 and 20, “Were there any aspects of [morning/afternoon] training you found particularly useful or important? Please explain.”

9 Lessons Learned

As noted in Section 4.3 “Future Challenges” of this report, there is great value and need for the NSF CI community to share experiences and lessons learned within the community in an effort to strengthen preparedness and overall cybersecurity for NSF projects. In this section we document noteworthy observations of “lessons learned” during the 2017 Cybersecurity Summit.

In Todd Tannenbaum’s talk "Concerns and questions that should keep software creators awake at night" he points out that when a security bug is found in software, always search for more

instances of the same problem. The reusability of code can result in propagating security flaws.

Evan F. Bolling from the Minnesota Supercomputing Institute (MSI) shared a number of experiences in this talk "From Bare Metal to Virtual: Lessons Learned when a Supercomputing Institute Deploys its First Cloud". Evan noted that it's easy to point fingers at others rather than taking ownership of an issue. Staff culture can be resistant to change and new responsibilities. Taking ownership and communication are key to changing staff culture. Dispelling the risks to staff, and clearly stating that these new roles won't cost them their job, result in personal financial liability, or lead to prison time can help ease their concerns. He also suggested emphasizing new responsibilities as professional development for staff and/or co-authorship in research papers to advance their careers. He also pointed out that Openstack is a hot skill set in the current market, making those with experience more attractive to employers. Finally MSI found that the NIH Genomic Data Sharing (GDS) Policy policy is lax, but that the dbGaP best practices policy is a good checklist that can be expanded later.

During the Cloud Security panel it was highlighted that standards must evolve over time to adjust to the changing environment, and in some cases to correct past guidance. For example in August of 2017 NIST revised special publication 800-63-3 "Digital Identity Guideline"[8] <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-63ver1.0.1.pdf> relaxing password complexity requirements and increasing password lengths. The password expiration guideline was removed completely and the new guideline directs that passwords should only change if it has been stolen, exposed, or hacked.

10 Conclusion

We were pleased with the introduction of the theme *"Ensuring Data Provenance, Integrity and Resilience"* and the impact it generated for this year's summit. We believe the theme provided a strong motivating force that tied together the keynotes and presentations and helped focus the community into sharing experiences on a particular topic that we and the community deemed relevant. Moreover, it is encouraging that the community participants and response to call for proposals increased for the third straight year. To this end, we thank the community members who helped the summit achieve its goals. In particular, we thank those who served on the program committee for their effort and devotion to the summit.

We are excited for next year's summit and for the opportunity to confront new cybersecurity challenges in our unique and collaborative environment. This will require, however, that we,

[8] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

the program committee, and the community continue to be vigilant in identifying new and relevant areas for discussion at next year's summit. And as always, we will continue to evolve and improve upon the summit to adapt to the community's changing needs, e.g., adjusting our registration model to expand participation by the NSF and broader communities.

Finally, we thank the NSF for funding the summits and providing presentations.

Appendix A: Recommendations for Past Summits

This appendix serves as a compendium for all recommendations made in past summit reports. The exact role of these "recommendations" has shifted over time, with some recommendations being directly carried over from year-to-year, while others were rebranded as "Opportunities," and others may be tweaked or responded to. Despite this changing usage, this appendix should provide a comprehensive perspective of the takeaways from past summits, and should serve to inform recommendations made in this and future summit reports.

2016 Recommendations:

Note: the 2016 Summit Report carried over the Recommendations from the 2015 Report.

Recommendation 1: The NSF CI and Large Facility community should develop a broadly applicable strategy for information security budgets, including how, why, and where it does what it does in terms of spending.

Recommendation 2: The NSF CI and Large Facility community should support research on metrics that indicate whether spending on information security is sufficient and appropriately balanced with a project's science mission.

Recommendation 3: The NSF CI and Large Facility community should develop a common understanding among all stakeholders of how accountability, risk responsibility, and risk acceptance practices are most efficiently and appropriately distributed among project leadership, project personnel, and other stakeholders.

Recommendation 4: The NSF CI and Large Facility community should determine its software assurance, quality, and supply chain requirements.

Recommendation 5: Utilizing a consensus process that includes all stakeholders, the NSF CI and Large Facility community should adopt a common, broadly applicable framework for information security.

Recommendation 6: The NSF CI and Large Facility community should continue to implement, refine, and evaluate risk-based approaches to cybersecurity that leverage established best practices as much as possible, while also addressing the community's particular needs around unique scientific instruments, data, openness, multi-organizational relationships, mission assurance, resilience, and project lifespans.

Recommendation 7: The NSF CI and Large Facility community should find more ongoing ways of collaboratively developing and maintaining cybersecurity programs, such as sharing

materials, services, practices, lessons learned, and collaborative/peer reviews.

Recommendation 8: The NSF CI and Large Facility community should continue to develop and disseminate best practices for identity and access management to support research.

Opportunity 1: The NSF CI and Large Facility community should explore how it can 12 support, participate in, and directly benefit from basic and applied cybersecurity research like that funded via NSF's Secure and Trustworthy Cyberspace (SaTC) and Risk and Resilience solicitations.

Opportunity 2: The NSF CI and Large Facility community should closely follow, 13 participate in, evaluate, and validate the NSF Cybersecurity Center of Excellence's community threat model development effort, including determining whether insights into threat actors and threat events positively impact the efficiency and effectiveness of our cybersecurity programs and risk management processes.

Opportunity 3: The NSF CI and Large Facility community should explore collaboration 14 with, and even drive change in, existing cross-organizational mechanisms (e.g., REN-ISAC, EDUCAUSE, Internet2) where information sharing can efficiently and effectively help the community gain a defensive advantage.

Opportunity 4: The NSF CI and Large Facility community should determine when and 15 how privacy intersects with NSF CI cybersecurity efforts in terms of (i) legal and regulatory requirements; (ii) our community's norms, values, and stakeholder relationships; and (iii) being a barrier to and/or enabler of science

2015 Recommendations:

Recommendation 1: The NSF CI and Large Facility community should develop a broadly applicable strategy for information security budgets, including how, why, and where it does what it does in terms of spending

Recommendation 2: The NSF CI and Large Facility community should support research on metrics that indicate whether spending on information security is sufficient and appropriately balanced with a project's science mission.

Recommendation 3: The NSF CI and Large Facility community should develop a common understanding among all stakeholders of how accountability, risk responsibility, and risk Report of the 2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure 16 acceptance practices are most efficiently and appropriately distributed among project

leadership, project personnel, and other stakeholders.

Recommendation 4: The NSF CI and Large Facility community should determine its software assurance, quality, and supply chain requirements.

Recommendation 5: Utilizing a consensus process that includes all stakeholders, the NSF CI and Large Facility community should adopt a common, broadly applicable framework for information security.

Recommendation 6: The NSF CI and Large Facility community should continue to implement, refine, and evaluate risk-based approaches to cybersecurity that leverage established best practices as much as possible, while also addressing the community's particular needs around unique scientific instruments, data, openness, multi-organizational relationships, mission assurance, resilience, and project lifespans

Recommendation 7: The NSF CI and Large Facility community should find more ongoing ways of collaboratively developing and maintaining cybersecurity programs, such as sharing materials, services, practices, lessons learned, and collaborative/peer reviews.

Recommendation 8: The NSF CI and Large Facility community should continue to develop and disseminate best practices for identity and access management to support research.

Recommendation 9: The NSF CI and Large Facility community should determine when and how privacy intersects with NSF CI cybersecurity efforts in terms of (i) legal and regulatory requirements; (ii) our community's norms, values, and stakeholder relationships; and (iii) being a barrier to and/or enabler of science.

Recommendation 10: The NSF CI and Large Facility community should explore how it can support, participate in, and directly benefit from basic and applied cybersecurity research like that funded via NSF's Secure and Trustworthy Cyberspace (SaTC) and Risk and Resilience solicitations.

Recommendation 11: The NSF CI and Large Facility community should closely follow, participate in, evaluate, and validate the NSF Cybersecurity Center of Excellence's community threat model development effort, including determining whether insights into threat actors and threat events positively impact the efficiency and effectiveness of our cybersecurity programs and risk management processes.

Recommendation 12: The NSF CI and Large Facility community should explore collaboration with, and even drive change in, existing cross-organizational mechanisms (e.g., REN-ISAC, EDUCAUSE, Internet2) where information sharing can efficiently and effectively help the

community gain a defensive advantage.

2014 Recommendations:

Recommendation 1: The NSF CI and Large Facility community should define its own best practices for cybersecurity rather than anticipating detailed direction from NSF. Clearly setting our own standards will help protect us from compliance directives not as well-suited to our community.

Recommendation 2: The NSF CI and Large Facility community should implement a risk-based approach to cybersecurity that leverages broader best practices as much as possible, while addressing and balancing the community's particular needs around unique scientific instruments, data, openness, multi-organizational relationships, and project lifespans.

Recommendation 3: The NSF CI and Large Facility community should identify and share best practices for how to successfully integrate security throughout and across project organizations.

Recommendation 4: The NSF CI and Large Facility community should develop a common understanding of how risk responsibility and acceptance practices are most efficiently and appropriately distributed among project personnel and stakeholders.

Recommendation 5: The NSF CI and Large Facility community should explore ways of collaboratively developing and maintaining cybersecurity programs, such as sharing materials, services, policies, practices, lessons learned, and collaborative/peer reviews.

Recommendation 6: The NSF CI and Large Facility community should continue to find ways of sharing real-time data in order to foster continuity of expertise and gain as much of an advantage as possible in defending ourselves. Existing cross-organizational mechanisms (e.g., REN-ISAC, EDUCAUSE, Internet2) should be evaluated in terms of how they could be leveraged.

Recommendation 7: We recommend the NSF CI and Large Facility community undertake or support a research effort to increase understanding and communicate that knowledge or know-how for each of the following open questions:

D. What is the threat profile for our community, and can insights into threat actors and their motivations positively impact the efficiency and effectiveness of our cybersecurity programs and risk management processes?

E. When and how does privacy intersect with NSF CI cybersecurity efforts in terms of (i)

legal and regulatory requirements; (ii) our community's norms, values, and stakeholder relationships; and (iii) being a barrier to and/or enabler of science?

F. How do we include and meaningfully address software assurance, quality, or supply chain in the context of the project cybersecurity programs, and the summit itself?

2013 Recommendations:

(Recommendation) 1: The community should identify a means to organize future summits.

(Recommendation) 2: Future summits should continue to include NSF project principal investigators, other key stakeholders and risk owners to ensure that NSF cybersecurity evolves to address their needs.

(Recommendation) 3: Future program committees should consider more time and opportunities (e.g., increased seating) for tutorials, hands-on activities, and organized discussion.

(Recommendation) 4: Future program committees should take on gender, age, and racial/ethnic diversity in the community and the summit attendance as a strategic imperative for future summits.

(Recommendation) 5: The community should consider the relationship between large facilities and smaller cyberinfrastructure projects, and their potential synergies around cybersecurity, as well as how (and if) the summit can effectively address both.

(Recommendation) 6: The community needs to develop a better understanding of the expectations for their cybersecurity programs and how to meet those expectations.

Appendix B: Call For Participation

Call for Participation

2017 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

August 15-17 * Westin Arlington Gateway * Arlington, VA

Theme: ***Ensuring Data Provenance, Integrity and Resilience***

It is our great pleasure to announce that the 2017 Summit will take place Tuesday, August 15th through Thursday, August 17th, at the Westin Arlington Gateway near the National Science Foundation Headquarters in Arlington, VA. On August 15th, the Summit will offer a full day of information security training tailored for the NSF community. The second and third days will follow a workshop format designed to increase the NSF community's understanding of cybersecurity strategies that strengthen trustworthy science: what data, processes, and systems are crucial to the scientific mission, what risks they face, and how to protect them.

About the Summit

Since 2004, the annual NSF Cybersecurity Summit has served as a valuable part of the process of securing the NSF scientific cyberinfrastructure by providing the community a forum for education, sharing experiences, building relationships, and establishing best practices.

The NSF cyberinfrastructure ecosystem presents an aggregate of complex cybersecurity needs (e.g., scientific data and instruments, unique computational and storage resources, complex collaborations) as compared to other organizations and sectors. This community has a unique opportunity to develop information security practices tailored to these needs, as well as break new ground on efficient, effective ways to protect information assets while supporting science. The Summit will bring together leaders in NSF cyberinfrastructure and cybersecurity to continue the processes initiated in 2013-2016: Building a trusting, collaborative community, and seriously addressing that community's core cybersecurity challenges.

The Summit seeks proposals for presentations, breakout and training sessions. It offers opportunities for student scholarships.

Proposing Content for the Summit

There are many ways to contribute to the Cybersecurity Summit. We are open to proposals for full- or half-day training sessions, for plenary presentations, and for breakout sessions. More specific information on each of those is available below. Submissions should be sent to CFP@trustedci.org by June 5th. Responses should go out by June 26th to ensure adequate planning time for presenters.

Proposing a Plenary Presentation

Please submit brief white papers focused on NSF Large Facilities' unmet cybersecurity challenges, lessons learned, and/or significant successes for presentation during the Summit Plenary Session (Aug 16-17). White papers (and presentations) may be in the form of position papers and/or narratives and may be one to five pages in length.

All submitted white papers will be included in the 2017 summit report. The Program Committee will select the most relevant, reasoned, and broadly interesting for presentation. A limited amount of funding is available to assist with travel for accepted submissions.

Submission deadline: June 5th

Submit to: CFP@trustedci.org

Word limit: 400 to 2000 words (~1-5 single spaced pages)

Notification of acceptance: June 26th

Proposing a Training Session

Training may be targeted at technical and/or management audiences, and be half-day or full-day in length. Areas of interest include, but are not limited to: cybersecurity planning and programs, risk assessment and management, regulatory compliance, identity and access management, data management and provenance, networks security and monitoring, secure coding and software assurance, physical security in the context of information security, and information security of scientific and emerging technologies. The Program Committee will select the most community-relevant and broadly interesting training sessions for presentation during the first day of the summit (Aug 15).

We generally prefer training sessions with some hands-on or interactive component over those that can be equally well presented in a non-interactive format (e.g. online videos), whether that component is a series of review Q&As, the opportunity to work directly with a piece of software or other tool, or a planning/management activity.

Submission deadline: June 5th

Submit to: CFP@trustedci.org

Word Limit: 600 words

Notification of Acceptance: June 26th

Proposing Table Top Sessions

In past years, the Summit has experimented with other formats for networking and information exchange, such as table-top topics at lunch. Proposals for such an activity should be 1-2 pages in length and include who would run the activity, the activity's intended audience, and a description of the activity itself and its expected benefits.

Submission deadline: June 5th

Submit to: CFP@trustedci.org

Word limit: 400 to 800 words (~1-2 single spaced pages)

Notification of acceptance: June 26th

Information for Students

Each year, the summit organizers invite several students to attend the summit. Reimbursement of travel expenses may be available. See http://trustedci.org/students2017/ for more information.

Notes for First-Time Presenters

The Summit organizers want to encourage those who have not presented at previous Summits to share their experiences, expertise, and insights with the NSF cybersecurity community. You don't need to be perfectly polished, you just need to have something to share about your project or facility's experience with information security. Feedback from last year's Summit showed that there was a great deal of interest in "lessons learned" type presentations from projects who've faced cybersecurity challenges, and had to rethink some things afterwards. We've put together a page of tips and ideas for new presenters, including proposal and presentation tips as well as suggested topics. More direct coaching is available upon request.

Please contact CFP@trustedci.org with any questions, or to request help preparing a proposal or getting it ready to present at the Summit.

So you want to present at the 2017 NSF Cybersecurity Summit...

Welcome! The Summit organizers wish to encourage and support participation from throughout the wider NSF community. To further that mission, we've provided some information (below) to aid in the preparation of CFP responses. Please don't hesitate to direct questions to CFP@trustedci.org.

What to Present

This year's theme is "Ensuring Data Provenance, Integrity and Resilience." This is a subject that is the underlying motivation for all of the cybersecurity activities we pursue. The organizers especially appreciate proposals that drive this home, however, not every presentation, training session, or activity has to be centered around just that topic. Please submit any idea that you think may be relevant to our audience. If you would like to present, but aren't sure of what topic to choose, consider the following suggestions:

- Lessons Learned: Get beyond the brag session. Tell the audience about something that DIDN'T go well for your project's cybersecurity efforts and how you overcame it. Even if you haven't overcome it yet, share the questions you are struggling with and open things up to the audience for Q&A or brainstorming. Too often, those doing cybersecurity in our community only see the big successes that others do press releases about, but there is even more to learn about the things that don't work.
- Tools: Have you discovered a new or unusual tool or technique that enables you in

cybersecurity work? Do a "getting started" tutorial to help others learn about it so that they can implement it for themselves.
- Enabling Cybersecurity Professional Development: What do you do to find, train, and retain good people? How do you enable them to keep their skills fresh and growing?
- It would be great to get a session on approaches to building the cybersecurity workforce available to the science community.

We strongly encourage proposals that address the 2016 Summit finding and recommendations:

- Information Security Budgets
- Accountability, Risk Acceptance, and the Role of Project Leadership
- Software assurance

More details on the recommendations can be found in the 2016 NSF summit report: https://scholarworks.iu.edu/dspace/handle/2022/21161

Additionally, the following ideas might help you build a presentation idea around this year's theme, or work the theme into your presentation's topic:

- Supply chain requirements
- What are your most valuable and/or sensitive data?
    - What assets have you had the most trouble protecting?
    - Where have you found the best resources? For commodity technologies? For your special equipment?
- Have you gone through a process of formally identifying your information assets for security purposes? What does the documentation look like? What challenges have you faced (e.g., in classifying data)?
- Did you find anything assets that surprised you…. that you didn't think of as critical to the integrity of the scientific results?
- How do you assign responsibility for / stewardship of specific information assets (or sets of assets that serve a process) within your organization? When if ever does security have direct accountability for the security of these assets?

How to Build a CFP Response

The proposal you submit will be used in two ways: to tell the organizers about what you plan to present, and to be included in the summit findings as a sort of after-action report. It should include:

- An executive summary (short description of the topic and content).
- Who the presenter(s) is/are.
- Either a whitepaper discussion of the topic, or a narrative you'd like to share with the community. (For activities that are not trainings or plenary sessions, this may be replaced with a description of the planned activity, any space or equipment needs, and the activity's intended audience.)
- Contact information (preferably email) for the presenter(s) in case the organizers have any questions. This can be in a separate note in the email body instead of the proposal itself if presenter(s) don't wish it to be published.
- Expected length of the session/training/activity. Generally, trainings are either full- or half-day and plenary sessions are about 50 minutes, but if a good idea takes more time than that, we will work with presenters to make it happen.
- Any relevant references (e.g. link to the home page for the project the talk is about, or recommendations for further reading).

Our community has expressed in the past that many find it helpful if they can download a copy of a presentation's slides. If you are willing to publish your slides, please email a copy (or a link to where you prefer to host slides) to CFP@trustedci.org.

The easiest way to get help/feedback from the organizing committee prior to submitting your final proposal is to create a Google Doc containing your proposal and sending an edit link to CFP@trustedci.org. Don't share directly with that address, as the link will be passed on to a reviewer who will have their own google account.

Tips for Presenting

There are many different presentation formats that can work well, depending on the topic. Consider the following:

- **Lecture format:** The presenter(s) talk to the audience and show slides to support their dialogue, then do a short Q&A time at the end of the presentation.
- **Panel format:** 3-5 persons answer questions offered by a moderator on a specific topic or set of topics, then do a short Q&A with the audience. This tends to work out best when the panel contains people with very different backgrounds or viewpoints, and the moderator is good at keeping folks to the topic and time constraints.
- **Open Forum format:** 2-3 persons answer questions offered by the audience. Works best if there is an extra person gathering questions and presenting them, and if the speakers can keep things succinct so that the presentation keeps moving and many

questions get answered.

- **Hands-on format:** The presenter(s) walk the audience through a demo or tutorial as the audience follows along on their computers (or on paper, if the topic supports it). If you are doing a training that will have many hands-on activities, consider having more than one presenter, or a presenter plus a helper or two who can go around the room and help participants who get stuck, allowing the group as a whole to move on.

Whatever format you choose, be sure to engage your audience by making eye contact (with them, not with the slide screen!), showing interest in what you are saying, and not rushing. Most speakers appear most smooth and practiced when following a general outline they've practiced once or twice, rather than trying to read a prepared script verbatim.

Appendix C: Descriptions of Training Sessions

Concurrent Morning Sessions

WISE Workshop (Full Day)

Instructors: WISE Community

The WISE (Wise Information Security for collaborating E-infrastructures) community was born as the result of a workshop in October 2015, which was jointly organized by the GÉANT group SIG-ISM (Special Interest Group on Information Security Management) and SCI, the 'Security for Collaboration among Infrastructures' group of staff from several large-scale distributed computing infrastructures. All agreed at the workshop that collaboration and trust is the key to successful information security in the world of federated digital infrastructures for research. WISE is an international community with participants spanning North America, Europe, Asia and Australasia.

WISE provides a trusted global framework where security experts can share information on topics such as risk management, experiences about certification processes and threat intelligence. With participants from e-Infrastructures such as EGI, EUDAT, GEANT, PRACE, XSEDE, OSG, NRENs and more, WISE focuses on standards, guidelines and practices, and promotes the protection of critical infrastructure. To date WISE has created four working groups, each tackling different aspects of collaborative security and trust. The community is currently working on defining a comprehensive security training catalogue (STAA-WG), risk assessment template (RAW-WG), big data best practice guidelines (SBOD-WG) and guidance for assessing an infrastructure against the new version 2 of SCI, the framework established to ease cross-infrastructure information exchange during security incidents (SCIv2-WG).

We invite security representatives from E-Infrastructures to participate. This includes operations security individuals and policy makers.

Additional information can be found at: https://wiki.geant.org/display/WISE/WISE+@+NSF+Summit

Federated Identity Management for Research Organizations

Instructors: Jim Basney (NCSA and University of Illinois/CTSC) and Scott Koranda (Spherical Cow Group/CTSC)

Research Organizations and Collaborations, and especially Virtual Organizations (VOs), come together to solve complex problems leveraging people and resources from multiple institutions, often spanning the world. Expert in their respective domains, VOs rarely have expertise in the identity management aspects of collaboration. Regardless of VO size, properly designed identity management processes and technologies can help facilitate VO research by providing access to collaboration tools and services quickly, and removing that access when it should no longer be granted.

This full-day tutorial will provide an overview of the issues in identity management facing and solutions available to VOs, in order to help them more easily manage access to their resources.

Topics covered will include:

- Understanding the identity management process needs of VOs of any size
- Leveraging Federated and Social Identity to authenticate VO participants
- Understanding the complexities of international federation and collaboration
- Passwords, Certificates, SSH Keys, and other authentication technologies: what works

where?
- Participant lifecycle management using open source identity management solutions, including COmanage, Grouper, and Shibboleth
- Application Integration and Provisioning, from the shell to the web to the cloud: how to make apps work with identity management infrastructure
Interactive demonstrations will be used to provide tangible insight into the capabilities of various solutions.
Note: A previous version of this training was given at the 2016 NSF Cybersecurity Summit.

Security Log Analysis

Instructor: Mark Krenz (Indiana University/CTSC)
The goal of security log analysis is to more efficiently leverage log collection in order to identify threats and anomalies in their cyberinfrastructure. I will be presenting a half-day training that will help attendees tie various log and data sources together to provide a more rounded, coherent picture of a potential security event. It will also help attendees understand log analysis as a life cycle (Collection, Event Management, Analysis, Response) that continues to become more efficient over time. It will demonstrate how proper management of these four phases contributes to a security team's effectiveness. Interactive demonstrations will cover both automated and manual analysis using multiple log sources (network protocols, files, software, intel, etc.), with examples from real security incidents. Lastly, the training will cover how to use lessons learned during each cycle to tune the monitoring and analysis workflow to improve an organization's operational security footing over time.

Legacy Industrial Control Systems - Secure / Replace / Ignore?

Instructor: Phil Salkie (Jenariah Industrial Automation)
Scientific and technical facilities worldwide incorporate Programmable Logic Controllers (PLCs) and Supervisory Control And Data Acquisition (SCADA) systems into their mix of technologies - often without the knowledge or support of the on-site IT department. These systems can include decades-old designs, contain firmware which is not (or cannot) be updated or patched, and can have long lists of known vulnerabilities - yet they continue to be placed into network environments throughout the world. This breakout session will provide a framework for IT department management to inventory, evaluate, triage, and secure their existing controls systems, as well as supplying specification language for use when systems must be replaced with modern, security-aware hardware.

Handling Regulated Government Data, Protected Health Information, and CUI

Instructor: Anurag Shankar (Indiana University)
With cyber threat at unprecedented levels, the May 11th presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure requires government agencies to examine unmet cybersecurity needs and take appropriate actions to protect the nation and the public at large. Downstream effects are likely to follow for government subcontractors, especially R&D facilities and academia, already in a difficult position due to insufficient resources, regulatory expertise, and often the

presence of both government information subject to FISMA and "Controlled Unclassifed Information" (CUI), for instance HIPAA protected health information (PHI). Each data type requires adherence to different standards – the NIST Risk Management Framework (RMF) and NIST 800-53 controls for FISMA, the recently released NIST SP 800-171 controls for CUI, and HIPAA Security Rule safeguards for PHI. This workshop is designed to untangle these different data types, regulations, and requirements, and to provide guidance on how to build and deploy an effective cyber risk mitigation strategy that enables one to handle compliance and bolster cybersecurity in the most cost-effective way.

Digital Forensics / Incident Response

Instructor: Warren Raquel (NCSA and University of Illinois/CTSC)

Digital forensics can provide a deeper understanding of what happened during a Cybersecurity event than what standard incident response measures can provide. If you are considering adding digital forensics capabilities to your Cybersecurity program this program will walk through what you will need to do this. We will discuss how to start small and build up your capabilities. At the end of this program you should understand the pros and cons of a digital forensics program and how to get it off the ground.

Computer incident response is a required capability for any project or activity that is running internet connected services. CTSC would present a half-day tutorial that will provide basic information on setting up an incident response program so that students can prepare their project team or organization for an incident investigation. The initial focus of the tutorial will be on identifying the processes, policies, information, and monitoring services that are required to effectively respond to a security incident. This first section will discuss investigation and analysis tools that might be useful for investigations. The second part of the tutorial will identify a series of questions the incident response team can use to guide them through both the investigation and the mitigation process. The participant should leave the session with an understanding of the basic steps needed to create an incident response program and what to do when an incident occurs.

Concurrent Afternoon Sessions

WISE Workshop (continued)

See full description above.

Federated Identity Management for Research Organizations (continued)

See full description above.

Shared Intelligence Platform for Protecting our National Cyberinfrastructure

Instructor: Alex Withers (NCSA / University of Illinois)

The SDAIA project seeks to advance the security infrastructure available for open science networks, aka Science DMZs. This research is expected to significantly enhance the security of campus and research networks. It addresses the emerging security challenge of open, unrestricted access to campus research networks, but beyond that it lays the foundation for an evolvable intelligence sharing network with the very real potential for national scale analysis of that intelligence. Further it will supply cyber security researchers

with a rich real-world intelligence source upon which to test their theories, tools, and techniques. The research will produce a new kind of virtual security appliance that will significantly enhance the security posture of open science networks so that advanced high-performance network-based research can be carried out free of performance lags induced by more traditional security controls.
More than just a VM running CIF, this appliance gives users the ability to build or join a data sharing network with their partners and share potential threat data within seconds. The appliance also provides a framework to stay ahead of threats as events get shared and to act on these events. The training will breakdown the virtual appliance into its individual components by having attendees deploy each component with Ansible. We will cover each component and its role in the appliance: ssh-auth-logger honeypot, zyre/zeromq for p2p sharing, cifv3 for event store and later analysis, bro for honeypot network analysis, bro's intel framework to stay ahead of potential threats, and components to allow integration into existing security monitoring infrastructure. We will demonstrate how components can be deployed in whole or part and orchestrated to suit an institution's data sharing needs.

Rebuilding a Plane in Flight: Refactors Under Pressure

Instructor: Susan Sons (Indiana University)

At some point, every engineer or project manager will have to take on a disaster. In these situations, it is easy to go into firefighting mode, trying to keep each new emergency at bay, instead of taking a systematic approach to fixing the underlying problems. This is why disgusting, brittle tangles of hundreds of thousands of lines of insecure spaghetti code stay in place so long. It is why you are inheriting a network of vulnerable SCADA components that the last four people were too afraid to fix.
Attempting to untangle a disaster that cannot be taken out of service is terrifying. Eventually, it must be done, but often no one wants to take responsibility for the project until it is almost too late. However, there is method to the madness. Susan Sons shares a high-level approach to safely refactoring software and other complex systems while supporting production deployments that may themselves be complex and varied, drawing from her experience refactoring life-critical software and cyber-physical systems (ICS/SCADA). While these methods were forged working on some critical systems and software, they apply just as well to a web application hairball or a DevOps nightmare.
Topics include:

- Project management concerns: Resourcing, outside communication, and staging changes
- Technical and architectural strategy: Supporting toolchains, triage, systems architecture, and refactor strategies
- Balancing response to immediate security and stability concerns against long-term vulnerability reduction and maintainability

Developing Cybersecurity Programs for NSF Projects

Instructors: Bob Cowles, Craig Jackson & Jim Marsteller (CTSC)

This instructional session will be based on a cybersecurity planning guide (see, trustedci.org/guide) developed with input from the Daniel K. Inouye Solar Telescope (DKIST) project, and in use at a number of NSF facilities and projects. The Guide was

developed to address the information security requirements outlined in NSF cooperative agreements, and provide solid guidance, tools, and resources. This session will be appropriate both for attendees of last year's training of the same name, as well as newcomers. Though there will be a good deal of overlap, we will be updating our presentation, and supporting opportunities to explore areas in greater depth based on participants' needs. Some of the topics that will be covered include:

- Building or Improving an Information Security Program
- Unique and Critical Science Requirements, Constraints, and Security Controls
- Information Security Policies and Procedures
- The Role of Project Leadership and Risk Acceptance
- Establishing a Risk Management Approach to Information Security
- Defining, Identifying, and Classifying Information Assets
- The Role of Risk Assessments within the Program Lifecycle
- Baseline Controls and Best Practices
- Topical Information Security Considerations: Third-Party Relationships, Asset Management, Access Control, Physical Security, Monitoring, Logging, and Retention
- Program Assessment and Evaluation

While this session will be instructional in nature, it is also intended to be an interactive session to seek constructive feedback from attendees to further improve the guide. There will be significant opportunities for discussion and Q&A.

Automated Assessment Tools - Theory & Practice

Instructors: Barton Miller & Elisa Heymann (University of Wisconsin / CTSC)

Software assurance tools – tools that scan the source or binary code of a program to find weaknesses – are the first line of defense in assessing the security of a software project. These tools can catch flaws in a program that can affect both the correctness and safety of the code. This tutorial is relevant to anyone wanting to understand how those tools work, and learn how to use these automated assessment tools to minimize security flaws in the software they develop or manage.

Description of the class:

We will introduce the different types of analysis tools, how these tools work, their output and their limitations. We then talk about control flow analysis and data flow analysis, as they are the tools' core to answer if certain code is safe or not.

The next section of the tutorial explain how to use different commercial and open source tools for C/C++ and Java, and how to process the tools' output. For that we use simple test applications extracted from the NIST/NSA Juliet test suite, where each of these applications contain specific weaknesses, and the version of the same code with the weakness fixed. The weaknesses we address are drawn from a collection of the most commonly occurring ones in real code, such as Relative Path Traversal, OS Command Injection, Cross-Site Scripting (XSS), Improper Neutralization of Script in an Error Message Web Page, Integer Overflow, Sensitive Information Uncleared Before Release, Uncaught Exception, and Use of Hard-coded Password.

Then we will move on to the hands-on section of this tutorial. The students will use the

Software Assurance Marketplace-SWAMP (https://continuousassurance.org/), which is an open facility that allows users to scan their software with different tools without the burden of dealing with tool acquisition, installation, and configuration. Throughout the SWAMP users can access both commercial and open source software assessment tools. By using the SWAMP the students will be able to identify problems in the given source code, modify the code, compile it, and submit it to the SWAMP for another assessment.

To attend this tutorial, you will need to:

1. Bring your own laptop.
2. Have VirtualBox installed on your machine.
1. Go to https://www.virtualbox.org/wiki/Downloads and download VirtualBox for your platform.
2. Execute the program downloaded.
3. Check that you are able to run VirtualBox.
3. For the class exercises, we will use two virtual machines images.

Please download them from:

www.cs.wisc.edu/mist/ctsc-ubuntu-1.ova (4.02 GB)

and

www.cs.wisc.edu/mist/ctsc-ubuntu-2.ova (4.3 GB)

Save them on the local disk of the machine you will be using for the tutorial. If you have problems downloading these images, we will have copies at the class.
If you have any questions before the tutorial, please contact elisa@cs.wisc.edu

Appendix D: Summit Agenda

Program Agenda

2017 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

August 15 - August 17 Westin Arlington Gateway Arlington, Virginia

https://trustedci.org/2017nsfsummit/

PC: Steve Barnet, Tony Baylis, Mike Corn, Rion Dooley, Barb Fossum, David Halstead, Ardoth Hassler, Susan Ramsey, George Strawn

Organizers: Diana Borecky, Leslee Bohland, Ryan Kiser, Mark Krenz, Jim Marsteller, Amy Starzynski Coddens, Von Welch

Training Day Tuesday

August 15, 2017

https://trustedci.org/2017training/

8:00am Registration and Continental Breakfast (Pre-Function Hemingway)

9:00am Morning and All Day Training Sessions Begin

- WISE Community: WISE Information Security for Collaborating E-Infrastructures
- Federated Identity Management for Research Organizations
- Security Log Analysis Training
- Legacy Industrial Control Systems - Secure / Replace / Ignore?
- Handling Regulated Government Data, Protected Health Information, and CUI
- Digital Forensics and Incident Response

11:00am ***Coffee Break***

11:30am Training Sessions Resume

1:00pm ***Lunch provided***

2:00pm Afternoon Training Sessions Begin and All Day Training Sessions Resume

- WISE Community: WISE Information Security for Collaborating E-Infrastructures
- Federated Identity Management for Research Organizations
- Shared Intelligence Platform for Protecting our National Cyberinfrastructure
- Rebuilding a Plane in Flight: Refactors Under Pressure
- Developing Cybersecurity Programs for NSF Projects
- Automated Assessment Tools - Theory & Practice

4:00pm ***Coffee Break***

4:30pm Training Sessions Resume

6:00pm Sessions End

Evening: ***Dinner on your own***

Plenary Session

Wednesday, August 16, 2017

F. Scott Fitzgerald AB

7:45am Sign-In and Continental Breakfast (Pre-Function AB)

8:30am Welcome and NSF Address (Jim Marsteller / Irene Qualters)

9:00am	***Keynote #1: Jeff Spies - "A Workflow-Centric Approach to Increasing Reproducibility and Data Integrity"***
10:00am	CCoE Update (Von Welch)
10:30am	***Coffee Break***
11:00am	From Bare Metal to Virtual: Lessons Learned when a Supercomputing Institute Deploys its First Cloud (Evan F. Bollig)
11:30am	Cornell Red Cloud: Campus-based Hybrid Cloud Computing
12:00pm	Panel: Cybersecurity in the Face of Overwhelming Threats Moderator: Von Welch (Indiana University, CTSC) Panelists: Michael Corn (UCSD) Anita Nikolich (NSF) Kim Milford (REN-ISAC)
1:00pm	Lunch and Table Topics - Lunch provided
2:30pm	HTCondor (Todd Tannenbaum)
3:00pm	Panel: Strategies to Develop a Diverse and Inclusive Cybersecurity Pipeline Moderator: Tony Baylis Panelists: Aurelia Williams (Norfolk State University) Victor Piotrowski (NSF) Rodney Petersen (NIST) Ambareen Siraj (Tennessee Tech University/WiCyS)
4:00pm	***Coffee Break***
4:30pm	Beyond the Beltway: The Problems with NIST's Approaches to Cybersecurity and Alternatives for NSF Science (Craig Jackson, Bob Cowles, Scott Russell)
5:00pm	Finding Your Way in the Dark: Security from First Principles (Susan Sons)
5:30pm	Open Discussion / Summary of the Day's Findings (Jim Marsteller / Von Welch)

6:00pm Dismissal

Plenary Session (continued)

Thursday, August 17, 2017

F. Scott Fitzgerald AB

7:45am Sign-In and Continental Breakfast (Pre-Function AB)

8:30am	***Keynote #2: Marjory Blumenthal - "Data, data, everywhere—how shall we live with it?"***
9:30am	Panel: Cloud Security & NSF Partnerships with Cloud Providers Moderator: Susan Ramsey Panelists: Susie Adams (Azure/Microsoft) Mark Ryland (AWS) Matthew O'Connor (Google)
10:30am	***Coffee Break***
11:00am	The Applicability of HPC for Cyber Situational Awareness (Leslie Leonard)
11:30am	Internet2 NOC Risk Assessment (Paul Howell)
12:00pm	Open Discussion / Summary of Summit Findings (Von Welch, Jim Marsteller)
12:30pm	Adjourn

Appendix E: List of Attendees and Organizations

Appendix F: WISE Workshop

WISE Feedback Gathered at the NSF Summit

This August, WISE was warmly welcomed to the NSF Cybersecurity Summit 2017 in Arlington, Virginia. Many thanks to our hosts for facilitating a hugely useful and productive workshop!

Doug Pearson from REN-ISAC kicked off the day with an interactive presentation of the pDNS Data Sharing project, aiming to pool anonymised passive DNS logs for the benefit of the R&E community. Our WISE colleagues were drafted in to play users, malicious DNS servers and the internet itself – to name but a few!

Florence Hudson from internet2 presented on the impact of IoT devices on security and sparked the question, "are there IoT devices in our e-Infrastructures?" This is one conversation that we will be taking forwards in the coming months to understand the impact of IoT security for WISE members.

Rob Quick from OSG took us "into the SWAMP" and demonstrated how we can assess common e-Infrastructure packages for security vulnerabilities in the SoftWare Assurance Market Place at http://mir-swamp.org/. This platform is open for the R&E community so don't hesitate to start analysing your own packages.

Alf Moens from SURF got our brains working as we performed a risk assessment exercise using WISE's newly published Risk Management Template. Participants gained a new found appreciation of the challenges faced when quantifying the risks faced by their organisations.

Dave Kelsey from STFC and Adam Slagel from XSEDE gathered feedback on SCIv2 from willing volunteers who had completed a first assessment of their e-Infrastructures in anticipation of the workshop. We were struck by the similarities with some of the work being done by CTSC, in both security frameworks and risk assessment, and will be working closely together to see how we can benefit each other's aims. The input received on SCIv2 during our day will be fed back into an FAQ to support future assessments… and help us all to be a little WISEr!

Appendix G: Bios for Speakers, Program Committee, and Organizers

Bios for Speakers, Authors, Program Committee Members, Organizers, and Student Awardees

In alphabetical order by surname

Susie Adams is the Chief Technology Officer for Microsoft's Federal Government business and brings with her over 30 years of IT experience. Susie joined Microsoft in 1999 and has held several leadership positions in Microsoft including the Director of the Microsoft Reston Virginia Technology Center and most recently the CTO of the Federal Civilian Business.

Prior to joining Microsoft, she spent 16 years in the consulting arena working with customers in both the commercial and government sectors. She held a variety of management and leadership roles including practice manager, systems analyst and software developer. Susie is a past Fed100 award winner and has authored several books on the topics of software integration and web development. Susie is a graduate of George Mason University where she received a BS in Information Systems.

*

Steve Barnet has specialized in supporting scientific and academic computing for nearly 20 years. During that time, he has worked in multiple domains including storage, networking, high-throughput computing, and security. He handled his first incident in 1995, a compromised Solaris system providing several important infrastructure services.

Steve currently works for the IceCube project, a kilometer scale neutrino detector located at the geographic South Pole. He began collaborating with CTSC in 2013 to develop a Cybersecurity plan for the IceCube facility.

*

Tom Barton is Sr Consultant for Cyber Security & Data Privacy at the University of Chicago and a consultant to Internet2. Previously he was Senior Director and Chief Information Security Officer at UChicago, and had earlier assignments as Director of IT Infrastructure and Director of Network Services at the University of Memphis, where he was a member of the mathematics faculty before turning to administration. He's a member of the Center for Trustworthy Scientific Cyberinfrastructure's Advisory Committee, the InCommon Federation's Technical Advisory Committee, the TIER Community Investors Council, the REFEDS Steering Committee, chaired the TIER Ad Hoc Advisory committee obsoleted by CACTI, and for many years led the Internet2 Grouper project.

*

Dr. Jim Basney is a senior research scientist in the cybersecurity group at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign. Jim's area of expertise is

identity management for scientific collaborations. He is PI of the CILogon and SciTokens projects and co- PI of the Center for Trustworthy Scientific Cyberinfrastructure and the Software Assurance Marketplace. Jim also contributes to the LIGO, LSST, and XSEDE projects. Jim received his PhD in computer sciences from the University of Wisconsin-Madison.

*

Tony Baylis is the senior management advocate for diversity and inclusion for the Laboratory. Tony is responsible for overseeing the laboratory's interactions and successful execution in building, partnering and collaborating with governmental, educational, industrial, community interests and other stakeholders. LLNL has had a long history in working with Minority Serving Institutions, specifically relationships with American Indian Institutions, Hispanic Institutions, and Historically Black College and Universities. He represents the Laboratory on the subjects of Diversity and Inclusion, STEM, Outreach Efforts, and Student Programs.

Tony's career represents 30 years of administrative, project, program, technical, and organizational management. He has worked in a scientific and technical environment for over 22 years and has worked as a consultant in industry as well. Tony has extensive experience networking with a broad range of academic, industry, government and non-profit organizations that has educated him and helped him in his career. He is a DOE Minorities in Energy Champion for the department and also serves on a number of conference program committees and advisory boards that promote STEM and diversity in science and technical careers.

*

Marjorie Blumenthal is a senior policy analyst and director of RAND's Science, Technology, and Policy Program. Prior to joining RAND, she served as executive director of the President's Council of Advisors on Science and Technology (PCAST) within the White House Office of Science and Technology Policy. Blumenthal's PCAST projects addressed how systems engineering can improve the delivery of health care, the challenge of protecting privacy in the context of big data, new directions for cybersecurity, how information technology can improve education and training, the implications of new technologies for cities, and more.

Previously Marjorie was an associate provost, academic at Georgetown University, developing academic strategy, strengthening the sciences and the overall research program, and promoting innovation in areas from international engagement to teaching and learning. Before starting at Georgetown, Blumenthal was the founding executive director of the National Academies' Computer Science and Telecommunications Board (CSTB). She convened and teamed with technologists, social scientists, and other experts, producing over 60 influential books and reports that addressed the full range of information technologies and their societal impacts. Blumenthal holds an M.P.P. from Harvard University.

*

Leslee A. Bohland serves as the Administrative & Finance Director at Indiana University's Center for Applied Cybersecurity Research (CACR). She is a graduate of the IU School of Business (B.S. '93). Leslee comes to the CACR and CTSC from a background in Management, Finance and Accounting. She has worked with government divisions, as well as in the private sector.

*

Evan Bollig, is a senior scientific computing consultant with the Minnesota Supercomputing Institute at the University of Minnesota. Evan is the lead architect, developer, and evangelist for Stratus, a research compute cloud for NIH controlled-access data. Since 2012, Evan has been integral to the creation of a number of cloud-based, clinically-certified (i.e., CLIA) data analysis pipelines used by Fairview Hospital's personalized medicine program. His other areas of interest include algorithm design on evolving HPC architectures (e.g., GPUs, FPGAs, and other accelerators), meshless numerical methods, and data visualization. Evan is a graduate of Florida State University (M.S. '09, Ph.D. '13), and proud alumnus of the NSF-funded SIParCS internship at the National Center for Atmospheric Research.

*

Diana Borecky serves as a Senior Administrative Asst. at Indiana University's Center for Applied Cybersecurity Research (CACR). She has worked for IU for 19 years in the IU UITS Finance office, before joining CACR staff.

*

Michael Corn is the CISO of the University of California at San Diego where he manages the Security Office as well as the Identity and Access Management. His areas of interest include privacy, identity management, and cloud services. He has been an active speaker and author on security and privacy and has participated in numerous Educause and Internet2 initiatives.

He is a member of the Internet2 Netplus Product Advisory Board and is the current co-chair of the Educause HEISC. Prior to joining UCSD he was the CISO & CPO and Deputy CIO of Brandeis University and was formally the CISO and Chief Privacy and Security Officer of the University of Illinois at Urbana- Champaign. He is a graduate of the University of Colorado at Boulder and the University of Illinois at Urbana-Champaign.

*

Robert (Bob) Cowles is a principal in BrightLite Information Security performing cybersecurity assessments and consulting in research and education about information security. He served as CISO at SLAC National Accelerator Laboratory (1997-¬2012); participated in the development of security policies and procedures for the LHC Computing Grid (2001-¬2008); and was an instructor at the University of Hong Kong in information security (2000¬-2003). A contributor to Indiana University's CACR since 2013, he participated in the XSIM project on identity management and has been working with CTSC since 2015. In 2017, he was honored to be named as a CACR Senior Fellow.

*

Dominique Dalanni is a senior attending George Washington University majoring in computer science, with a specialization in information assurance and cybersecurity. In addition to her studies, Ms. Dalanni is currently a participant in the Federal Pathways Internship Program, and interning with NIST. She is a CyberCorps scholarship recipient at George Washington University, the president of the Women in Stem Club, vice president and student advocate for the Com participant in the puting Alliance of Hispanic Serving Institutions (CAHSI) Club CSUDH chapter. She also served as a research assistant in a project

funded by the Nuclear Regulatory Commission and in 2015 was selected to represent her university as a CSU Trustee Award recipient and scholar.

After completing her undergraduate education, Ms. Dalanni hopes to pursue a graduate degree at George Washington University in Computer Science with a specialization in Cybersecurity. Once she has received her graduate degree, Ms. Dalanni would like explore job opportunities which focus on threat analysis, governance, or on the overall security of industrial control systems.

*

Rion Dooley is principal investigator on the Agave Project a Science-as-a-Service API platform allowing researchers worldwide to manage data, run code, collaborate freely, and integrate their science anywhere. His previous projects span areas of identity management, distributed web security, full-stack application development, data management, cloud services, and high performance computing. Rion earned a Ph.D. in computer science from Louisiana State University. Rion actively puts his wife and two daughters at the top of his list of accomplishments. He hopes his work can someday edge out dancing teddy bears and smear-proof lipstick on their lists of favorite inventions.

*

William Drake is the overnight supervisor for Indiana University's Data Center Operations department. He leads a team that is tasked with ensuring physical security at both of IU's data center facilities as well as monitoring the infrastructure that supports IU's enterprise and research computing systems. William is currently a student at IU pursuing a bachelor's degree at in informatics with a cognate in security informatics.

*

Barbara Fossum is a senior executive with over 25 years of leadership and management experience in higher academic and government sectors including high performance computing, data visualization, engineering and academic research. Barbara contributed several federally funded grants including the Network for Engineering Simulations where she successfully directed all operations and the development of a curated data repository for all earthquake engineering data. She is currently the CEO of BMF Consulting, providing extensive experience in human resource planning and operations, organizational change, team building, organizational effectiveness and facilitative leadership.

*

Nikita Golubets is a Student at Eastern Michigan University with a major in Information Assurance & Cyber Defense, Nikita Golubets finished his internship with the Security Solutions team at Cisco and will be graduating Spring of 2018. He had a chance to work with the TIP, CIRA, and Talos team and created an Automated Customer Attack Surface tool that gathers threat intelligence. He is a part of the National Cybersecurity Student Association that provides students with resources, mentors, as well as training in the field. Having a passion for the field, he attends Blackhat and Defcon security conferences and takes part in ISTS/ CCDC competitions.

*

Dr. David Halstead is the CIO for the National Radio Astronomy Observatory. After obtaining a PhD in

the computational simulation of surface catalysis in 1990, he moved to HPC research at the DOE Scalable Computing Laboratory in Ames Lab, implementing commodity parallel processing cluster solutions to benefit research in surface science, chemistry, physics and biology. In 2002 he moved into industry with Celera Genomics to drive the Strategic Platform Initiative; transitioning away from the costly leased computer systems used to sequence the human genome, to scalable HPC systems supporting proteomics and therapeutics research. Since joining NRAO in 2008, his responsibilities are divided between Data Management for the Observatory's HPC infrastructure in support of the national radio telescopes, and the general IT support for NRAO's 500+ employees. He has served on the committees for SC94, SC99, SC05, SC10; SC13; SC14; SC16 and is a founding member of the ACM's SIGHPC Education Chapter.

*

Ardoth Hassler retired in May as Associate Vice President of University Information Services at Georgetown University. Her work focused on policy, planning and research, including being the PI for NSF CC¬NIE and CC-IIE awards. In addition, she served as Interim Director of the Student Information Systems group.

Ardoth was on loan to the National Science Foundation 2007¬2011 where she served as Senior Information Technology Advisor in the Office of the Chief Information Officer in the NSF Office of Information and Resource Management, Division of Information Systems. Her activities included work related to cybersecurity best practices for large research facilities, working on technology policies for the Foundation and large research facilities, assisting NSF in joining the InCommon Federation and introducing concepts of single sign-on logon to Research.gov, leading the "SSN Be Gone" project to remove SSNs from FastLane and other systems where there was no business need, working on NSF's "Got Green", initiative, etc. She has prior experience serving on the program committees of the NSF Cybersecurity Summit, EDUCAUSE Annual Conferences, etc. She has a BS in Math (CS minor) from Oklahoma State University and an MS in Biostatistics from the University of Oklahoma.

*

Elisa Heymann is a Senior Scientist at the Computer Sciences Department of the University of Wisconsin-Madison, and an Associate Professor in the Computer Architecture and Operating Systems Department at the Autonomous University of Barcelona (UAB). She co-directs the MIST software vulnerability assessment project in collaboration with her colleagues at the University of Wisconsin. Heymann is part of CTSC, the NFS cyber security center for excellence, where she works on Software Assurance training and engagements.

Heymann carries out training in universities, companies, and conferences around the world. Heymann's research interests include security and resource management for Grid and Cloud environments, and cyber-security in transportation. Her research is supported by NSF, the Spanish government, the European Commission, and NATO. Heymann received her M.S. and Ph.D. degrees in Computer Science from the Autonomous University of Barcelona (Spain) in 1995 and 2001 respectively.

*

Paul Howell is Chief Cyberinfrastructure Security Officer at Internet2. Joining Internet2 in July, 2014, Paul oversees and coordinates all security efforts across the Internet2 infrastructure and is responsible for

setting organizational policies and approaches while engaging with the Internet2 member community. He is responsible for the creation and implementation of Internet2's information security program, advising on risk management and infrastructure; conducting security education, training, and awareness activities; monitoring compliance with security programs and applicable laws; and coordinating investigation and reporting of security incidents. Paul has more than 30 years of experience in IT security. In 2004, Paul was named The University of Michigan's Chief Security Officer. This was an inaugural role for the university, with Paul leading the development and implementation of the university's information assurance program.

*

Craig Jackson is Chief Policy Analyst at the Indiana University Center for Applied Cybersecurity Research (CACR), where his research interests include information security program development and governance, legal and regulatory regimes' impact on information security and cyber resilience, evidence-based security, and innovative defenses. He is a Co-PI of the NSF Cybersecurity Center of Excellence, and leads CACR's collaborative efforts with Naval Surface Warfare Center Crane Division. He is a graduate of the IU Maurer School of Law, IU School of Education, and Washington University in St. Louis. In addition to his litigation experience, Craig's research, design, project management, and psychology background includes work at the IU Center for Research on Learning and Technology and the Washington University in St. Louis School of Medicine.

*

Ryan Kiser is the Technology Specialist at the Indiana University Center for Applied Cybersecurity (CACR). Ryan comes to CACR from a system administration and small business consulting background. His current responsibilities include HIPAA compliance and risk assessment for university and external IT systems, managing the center's technical resources, as well as technical coordination and event planning.

*

Scott Koranda, PhD, specializes on identity management architecture for research organizations. Since 2008, Scott Koranda has designed, deployed, and supported production SAML infrastructures including both the Shibboleth Identity Provider (IdP) and Service Provider (SP) software, for the research and education sectors.

A member of the Laser Interferometer Gravitational Wave Observatory (LIGO) collaboration for over 10 years, Scott has served as the lead architect for the LIGO Identity and Access Management project since 2007. He was co-principal investigator on the NSF grant that funds COmanage development, and is a consultant with Spherical Cow Group.

*

Mark Krenz is the Lead Security Analyst at Indiana University's Center for Applied Cybersecurity Research with over two decades of experience in information security and system administration spread across multiple sectors. His interests at CACR include policy development, operational security development, security auditing and security education. He studied Computer Science and Mathematics at Indiana University.

*

Steven Lee joined Cornell University Center for Advanced Computing in 2007 as a systems consultant. In 2011, Steven helped to bring Red Cloud, a private research cloud with AWS-compatible API, into production to better accommodate workloads that do not fit into batch queues of HPC clusters.

He is currently working on Aristotle Cloud Federation, a federation of 3 research clouds at Cornell, University at Buffalo, and University of California Santa Barbara, to support scientists with flexible workloads and analysis tools for large scale data sets. Prior to Cornell, Steven worked as a systems and embedded software engineer in the telecommunications industry. He has a B.A. in computer science from Cornell University.

*

Leslie Leonard is the Cybersecurity Research Lead for the Department of Defense (DoD) High Performance Computing Modernization Program's (HPCMP) security team. The mission of the DoD HPCMP is to accelerate technology development and transition to superior defense capabilities, which provide DoD scientists and engineers with the resources necessary to solve the most demanding problems through the strategic application of high performance computing, high speed networks, and computational expertise.

Leslie leads Research and Development (R&D) for new technologies, tools, and techniques that enable the HPCMP to defend, mitigate, and secure five Defense Supercomputing Resource Centers (DSRCs) and the Defense Research and Engineering Network (DREN). She received her B.S./M.S. degrees in Computer Science from Jackson State University and a Ph.D. in Computer Science from the University of Maryland.

*

James A. Marsteller, Jr. is the Pittsburgh Supercomputer Center Chief Information Security Officer. He has extensive security leadership experience with the TeraGrid and XSEDE security operations team and is a Co-PI for the Center for Trustworthy Scientific Cyberinfrastructure, the NSF Cybersecurity Center of Excellence. James also has served as the program chair for annual NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure since 2007. He has also served on the board of directors for the Pittsburgh chapter of the FBI Infragard program for many years. He holds a Master of Information Technology Management from Carnegie Mellon University and is a Certified Information Systems Security Professional.

*

Kim Milford began serving as Executive Director of REN-ISAC in April 2014. She works with members, partners, sponsors, and advisory committees to direct strategic objectives in support of members, providing services and information that allow higher educational institutions to better defend local technical environments and is responsible for overseeing administration and operations.

Since joining Indiana University in June 2007, Ms. Milford has served in several roles leading strategic IT initiatives. As Chief Privacy Officer, she coordinated privacy-related efforts while serving on IU's Assurance Council, chairing the Committee of Data Stewards, and directing the work of the University

Information Policy Office including IU's IT incident response team. From 2005 – 2007, Ms. Milford worked as Information Security Officer at the University of Rochester leading an information security program that included disaster recovery planning, identity management, incident response, and user awareness. In her position as Information Security Manager at University of Wisconsin-Madison from 1998 - 2005, she assisted in establishing the university's information security department and co-led in the development of an annual security conference.

Ms. Milford provides cybersecurity, information policy, and privacy expertise and presentations at national and regional conferences, seminars and consortia. Ms. Milford has a B.S. in Accounting from Saint Louis University in St. Louis, Missouri and a J.D. from John Marshall Law School in Chicago, Illinois.

*

Barton Miller the Vilas Distinguished Achievement Professor and the Amar and Belinder Sohi Professor in Computer Sciences at the University of Wisconsin-Madison. He is Chief Scientist for the DHS Software Assurance Marketplace research facility. He co-directs the MIST software vulnerability assessment project in collaboration with his colleagues at the Autonomous University of Barcelona. He also leads Paradyn Parallel Performance Tool project, which is investigating performance and instrumentation technologies for parallel and distributed applications and systems. His research interests include systems security, binary and malicious code analysis and instrumentation extreme scale systems, parallel and distributed program measurement and debugging, and mobile computing.

Miller's research is supported by the U.S. Department of Homeland Security, U.S. Department of Energy, National Science Foundation, NATO, and various corporations. In 1988, Miller founded the field of Fuzz random software testing, which is the foundation of many security and software engineering disciplines. In 1992, Miller (working with then-student, Prof. Jeffrey Hollingsworth, founded the field of dynamic binary code instrumentation and coined the term "dynamic instrumentation". Dynamic instrumentation forms the basis for his current efforts in malware analysis and instrumentation.

Miller was the chair of the IDA Center for Computing Sciences Program Review Committee, a member of the Los Alamos National Laboratory Computing, Communications and Networking Division Review Committee, and has been on the U.S. Secret Service Electronic Crimes Task Force (Chicago Area), the Advisory Committee for Tuskegee University's High Performance Computing Program, and the Advisory Board for the International Summer Institute on Parallel Computer Architectures, Languages, and Algorithms in Prague. Miller is an active participant in the European Union APART performance tools initiative. Miller received his Ph.D. degree in Computer Science from the University of California, Berkeley in 1984. He is a Fellow of the ACM.

*

Sinjoni Mukhopadhyay is a second year PhD student pursuing a degree in Computer Science, with specialization in storage system security. She is a research assistant at the University’s Center for Research in Storage Systems. Sinjoni is currently working on possible alternatives to encryption for long term archives. Ongoing work includes efficient computations on secret-split datastores like patterns in reconstruction and secure searching. She is looking for internships for the summer of 2018, with

opportunities that will enhance her experience in the field of long-term secure archives. After completion of her program she hopes to explore job opportunities that will help her apply her expertise in providing better security alternatives for archival data.

*

Nicholas J. Multari provides programmatic and technical guidance to cybersecurity research programs at the Pacific Northwest National Lab (PNNL) including the multi-year lab directed research and development (LDRD) initiative focusing on Asymmetric Resilient Cybersecurity (ARC). In that role, he led the development of the multi-disciplinary research agenda required to provide a theoretical basis for, and the application of, technologies that reduce or eliminate a cyber-attacker's current asymmetric advantage. Prior to joining PNNL, he was the manager for trusted cyber technology at Boeing Research and Technology in Seattle, Washington. In that position, Nick directed and led a group of researchers conducting research, development, and technology assessment of cyber and cybersecurity technologies in support of Boeing Business Unit needs. In 2008, he served as a consultant to the USAF Scientific Advisory Board (SAB) investigating the effects of the contested cyber environment on the USAF mission.

Other positions held include five years as a Senior Security Engineer with Scitor Corporation in Northern Virginia, and 20 years as a computer scientist in the Air Force retiring as a Lt. Col. He is a member of external advisory boards at University of Washington and Iowa State University. He received a bachelor's degree in mathematics from Manhattan College, New York; a master's degree in computing and information science from Trinity University, Texas; and a PhD in computer science from the University of Texas at Austin.

*

Anita Nikolich is Program Director for Cybersecurity in the Division of Advanced Cyberinfrastructure at the National Science Foundation (NSF). Prior to her work at the NSF she served as the Executive Director of Infrastructure at the University of Chicago. Past assignments include Director of Global Data Networking at Aon and Director of Security for Worldcom. She has explored how information technology and secure networking can best support the creation and sharing of scientific knowledge in virtual, mobile and physical contexts. She holds a Master of Science from The University of Pennsylvania and a Bachelor of Arts from the University of Chicago.

*

Matthew O'Connor specializes in Security, Compliance, and (Anti)Abuse Products, on the Google Cloud Platform at Google. He serves in a CTO role for the Google Cloud Compliance Program, developing partnerships with Federal and private customers, and overseeing Managed Services. He attended Haas School of Business at UC Berkeley and obtained a BS in Computer Science Engineering from Santa Clara University.

*

Imani Palmer is a Ph.D. Candidate in the Department of Computer Science at the University of Illinois at Urbana-Champaign. Imani's areas of interest include cyber & systems security, digital forensics, and data analysis. She is a member of the Systems Research Group under the advisement of Roy Campbell.

She

received her B.S. in computer science from the University of Pittsburgh. After graduation, she is interested in a research position that allows her to continue to explore her interest in security.

*

Rodney Petersen is the director of the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce. He previously served as the Managing Director of the EDUCAUSE Washington Office and a Senior Government Relations Officer. He founded and directed the EDUCAUSE Cybersecurity Initiative and was the lead staff liaison for the Higher Education Information Security Council.

Prior to joining EDUCAUSE, he worked at two different times for the University of Maryland - first as Campus Compliance Officer in the Office of the President and later as the Director of IT Policy and Planning in the Office of the Vice President and Chief Information Officer. He also completed one year of federal service as an Instructor in the Academy for Community Service for AmeriCorps' National Civilian Community Corps. He is the co-editor of a book entitled "Computer and Network Security in Higher Education". He received his law degree from Wake Forest University and bachelors degrees in political science and business administration from Alma College. He was awarded a certificate as an Advanced Graduate Specialist in Education Policy, Planning, and Administration from the University of Maryland.

*

Victor Piotrowski is responsible for several programs related to Cybersecurity Education and Workforce Development. In particular, he oversees the CyberCorps(R): Scholarship for Service (SFS) program with FY2014 budget of $45 million. This program seeks to increase the number of qualified students entering the field of cybersecurity and to increase the capacity of the United States higher education enterprise to continue to produce professionals in this field to meet the needs of our increasingly technological society.

He is also a Program Officer in a NSF-wide program Secure and Trustworthy Cyberspace (SaTC) supporting projects that address cybersecurity from one or more perspectives: Trustworthy Computing Systems; Social, Behavioral and Economics; and Cybersecurity Education.

Before coming to NSF, Dr. Piotrowski served as a Professor and Chair of the Computer Science Department at the University of Wisconsin and as a faculty at the Institute of Informatics in Poland. He has a 20-year experience in research, teaching and consulting in Information Assurance and holds several cybersecurity certifications.

Dr. Piotrowski is the recipient of the Marcinkiewicz Prize by the Polish Mathematical Society and a finalist of the UW Board of Regents Teaching Excellence Award. He is a graduate of the Federal Executive Institute residency program Leadership for a Democratic Society and the Harvard Kennedy School Executive Education Cybersecurity Policy and Technology program.

*

Irene Qualters is the Division Director of the Division of Advanced Cyberinfrastructure at NSF. As a recognized leader in cyberinfrastructure infrastructure, she represents NSF in several interagency and international efforts that span software, data, and computation. For example, she has represented NSF in

the creation of the presidential initiative, NSCI.

Prior to her NSF career, Irene had a distinguished 30-year career in industry, with a number of executive leadership positions in the technology sector, in startups as well as a long tenure at Cray Research leading R&D, and six years with Merck Research Labs leading their Global Cyberinfrastructure for Research.

*

Susan Ramsey is a Risk Assessor and Security Engineer at the National Center for Atmospheric Research. She has over twenty years of experience building enterprise infrastructure and cloud computing. She joined NCAR in 2014 and promptly launched multiple initiatives to tackle compliance and identity management. Her latest projects include building a FISMA moderate segment and an organization wide Continuous Monitoring Plan. She has an MS in Computer Information Technology from Regis University, (thesis on Vulnerability Assessment). She is currently working towards a second Master of Science degree, in Information Security Engineering, from SANS Technical Institute.

*

Warren Raquel is a Senior Security Engineer at the National Center for Supercomputing Applications. His duties include security operations, incident response and security awareness for NCSA, Blue Waters and XSEDE. He has given talks and taught classes on Digital Forensics and Incident Response, two fields in which has specialized in for the last decade.

*

Scott Russell is a Senior Policy Analyst with CACR, where his work focuses on the improvement of federal cybersecurity standards. A lawyer and researcher, Scott specializes in privacy, cybersecurity, and international law, and his past research has included cybersecurity due diligence norms under international law, cybersecurity self-governance, international data jurisdiction, and constitutional issues on digital surveillance. Scott received his B.A. in Computer Science and History from the University of Virginia, received his J.D. from Indiana University, interned at MITRE, and served as a postdoctoral fellow at CACR.

*

Mark Ryland is the technology leader for Amazon Web Service's Worldwide Public Sector (WWPS) team, reporting to the Vice President of WWPS. Mr. Ryland leads a team of Solutions Architects and Professional Services / Rapid Adoption Program Engineers who provide AWS technical evangelism, architectural guidance, knowledge transfer, technical training, and implementation services to government and education customers around the globe.

Mark also serves as a key interface between the WWPS team and the engineering, security, and compliance teams at AWS, ensuring that public sector customer requirements are front-and-center in product/service planning and roadmaps. Mark holds a JD from University of California Berkeley School of Law, and a BA in Philosophy from UC San Diego.

*

Phil Salkie is a computer scientist who has been working as an industrial controls and automation

engineer since 1984. His software and hardware designs serve sectors as diverse as food packaging, broadcast television, emergency power generation, water purification, sewage processing, surgical suture manufacture, biopharmaceuticals, specialty chemicals, laundry transport, semiconductor equipment manufacture, and nuclear power plant infrastructure. He is managing partner of Jeneriah Industrial Automation.

*

Anurag Shankar is a senior security analyst at Indiana University's Center for Applied Cybersecurity Research (CACR). His expertise includes regulatory compliance (HIPAA, FISMA, CUI) and cybersecurity risk management. He has helped numerous institutions tackle HIPAA compliance and is responsible for developing a NIST based risk management framework and using it to align IU's central research and enterprise cyberinfrastructures with HIPAA. His prior engagements include nearly twenty years with IU's central IT organization developing, delivering, and managing Unix support, massive data storage, the national Teragrid project, and supporting the research mission of the IU School of Medicine. He played a key role in building IU's research data storage environments, for supporting IU's Indiana Genomics Initiative and other life sciences efforts, and for creating information infrastructures and technology solutions for the Indiana Clinical and Translational Sciences Institute (CTSI). He is a computational astrophysicist by training (Ph.D. University of Illinois, '90).

*

Rachel Shima, attending California State Polytechnic University.

*

Dr. Ambareen Siraj is currently serving as the Director of the Cybersecurity Education, Research, and Outreach Center at Tennessee Tech. She is also a Professor at the Computer Science department. Dr. Siraj's research areas of interest include smart grid security, sensor alert fusion with alert correlation and alert clustering, security metrics, security education and workforce development. She has authored/co-authored around forty journal and conference articles in these areas. She leads National Science Foundation Projects "Tennessee CyberCorps: A Hybrid Program in Cybersecurity", "Tennessee Tech Gen-Cyber Camps", "Capacity Building in Cybersecurity: Broadening Participation of Women in Cybersecurity through Women in Cybersecurity Conference & Professional Development", "CyberWorkshops: Resources and Strategies for Teaching Cybersecurity in Computer Science", and "Security Knitting Kit: Integrating Security into Traditional CS Courses". Dr. Siraj is the Founder and Chair of the Women in Cybersecurity (WiCyS) conference. She also leads the effort in establishment of the Middle Tennessee Cybersecurity Consortium (MTCC). She serves as the faculty advisor of Tech Cybersecurity Club for students.

*

Susan Sons serves as a Senior Systems Analyst at Indiana University's Center for Applied Cybersecurity Research, having come from a background in abuse management, software engineering, and pentesting. Susan considers herself a "generalist hacker" with specialties in ICS/SCADA security, secure software engineering, social engineering, and systems programming. Susan is President of the Internet Civil Engineering Institute (https://icei.org), a nonprofit dedicated to supporting and securing the common

software infrastructure we all depend on. Her recent publications have been with O'Reilly Publishing and Linux Journal. More on Susan's projects can be found at http://security.engineering.

*

Jeffrey Spies is the co-founder and Chief Technology Officer of the Center for Open Science (COS), a non-profit technology company missioned to increase openness, integrity, and reproducibility of scholarly research. He is also the co-director of SHARE, a partnership with the Association of Research Libraries to create a free, open data set of scholarly research activity across the research lifecycle. Jeff received his Ph.D. in Quantitative Psychology from the University of Virginia, where he now holds a Visiting Assistant Professor position in the Department of Engineering and Society. His dissertation included the development of the Open Science Framework (OSF)--a free, open source workflow management system and platform as a service that is now the flagship product of COS.

Jeff has a background in computer science and has conducted research in computational and statistical modeling as well as substantive domains including autism, non-verbal communication, and motor control. He continues to apply his research on scientific incentives, workflow, and reproducibility at COS and is regularly invited to speak on these topics. Jeff recently testified at a United States House congressional hearing on the role of openness and reproducibility in science.

*

Amy Starzynski Coddens serves as the Education, Outreach and Training Manager at Indiana University's Center for Applied Cybersecurity Research (CACR). She is a graduate of the IU School of Education (M.S. '06 & M.S. '09). Amy comes to the CACR and CTSC from a background in P-16 education and outreach. She has worked for the government, in industry and in academia, contributing to projects with the New England Research Institute, Harvard's PEAR Institute, the United States Department of Education's Office of Special Education Programs, NASA and the IU Kelley School of Business.

*

George O. Strawn is currently the director of the Board on Research Data and Information at the National Academies of Sciences, Engineering, and Medicine (having failed at retirement). Prior to joining the Academies, Dr. Strawn was the director of the National Coordination Office (NCO) for the Networking and Information Technology Research and Development (NITRD) Program and co-chair of the NITRD interagency committee. Dr. Strawn held these positions while on leave from the National Science Foundation (NSF) to the Office of Science and Technology Policy in the Whitehouse. Prior to his NITRD responsibilities, Dr. Strawn was the NSF Chief Information Officer. And prior to that, Dr. Strawn served in a number of capacities in the NSF Directorate for Computer and Information Science and Engineering (CISE). These included the executive officer of CISE, director of the CISE Division of Advanced Networking Infrastructure and Research, where he led NSF's efforts in the Presidential Next Generation Internet Initiative, and NSFnet Program Officer where he was part of the team that transitioned the experimental ARPAnet into the global Internet. Before to coming to NSF, Dr. Strawn was a Computer Science faculty member at Iowa State University (ISU) and a staff member in the Computation Center. He served terms as director of the Computation Center and as chair of the Computer

Science Department. Dr. Strawn received his Ph.D. in Mathematics from Iowa State University and his B.A. Magna Cum Laude in Mathematics and Physics from Cornell College. He is a fellow of the American Association of the Advancement of Science and a member of the Cosmos Club.

*

Todd Tannenbaum is a Researcher in the Department of Computer Sciences at UW-Madison with over 19 years of experience developing production distributed computing environments. He directs the development staff and serves as the Technical Lead for the HTCondor Project, a distributed computing research group that produces the award-winning HTCondor software. Previous to his involvement with HTCondor, Todd served as the Director of the Model Advanced Facility, a high-performance computing center in the UW-Madison College of Engineering, and also as a Technology Editor for Network Computing magazine. He received B.S. and M.S. degrees in computer science from UW-Madison.

*

Von Welch is the director of Indiana University's Center for Applied Cybersecurity Research (CACR) and PI for the NSF Cybersecurity Center of Excellence (CTSC). Additionally, he is the CISO of the Software Assurance Market Place, a DHS-funded facility to foster software assurance and software assurance research, and serves on the InCommon Steering Committee as an advisor for the research community. Previously he has worked with a range of high visibility projects to provide cybersecurity to the broader scientific and engineering community, including TeraGrid, Open Science Grid, Ocean Observatory Infrastructure, and GENI. His work in software and standards includes authoring two IETF RFCS and the contributing to the creation of the well-known CILogon and MyProxy projects.

*

Dr. Aurelia T. Williams is the Chairman and Professor of Computer Science at Norfolk State University (NSU). In this capacity, Dr. Williams manages oversight of two graduate programs in Computer Science and Cybersecurity and two undergraduate programs in Computer Science and Information Technology. As department chair and a member of the Cybersecurity team she has helped Cybersecurity at Norfolk State to grow across the departments at NSU, regionally and nationally. During her stewardship as chair of the Computer Science department, the Cybersecurity initiative has received 33 million dollars in Cybersecurity funding, received re-designation as a DHS/NSA Center of Academic Excellence in Cyber Defense Education, launched a MS Cybersecurity program and hosted the Vice President of the United States of America.

Dr. Williams is a successful manager and has been actively involved in Cybersecurity. Her research has focused on the application of Digital Forensics applied to Cloud Computing via the Information Assurance – Research, Education and Development Institute (IA-REDI), located at NSU, in addition to other aspects of Information Assurance and Security. She is the Principal Investigator of the department's award of $25M Consortium Enabling Cybersecurity Opportunities and Research (CECOR) where NSU leads a consortium of thirteen HBCUS and two DoE national laboratories to increase the workforce pipeline in Cybersecurity. She is a Co-PI of the NSF Scholarship for Service grant and has served as a mentor to students in the program. She is also a researcher on the Center of Excellence in Cybersecurity Research project. Dr. Williams uses these opportunities to serve as a research advisor to graduate and

undergraduate students completing their theses, projects and capstone courses.

Dr. Williams is a member of three professional and honorary societies. She volunteers in her community where she participates in various programs that promote the STEM (science, technology, engineering, and math) fields to students from elementary to college age. In addition to offering presentations on Cybersecurity topics to her peers and children, she was featured on the cover of BEHOLD, NSU's Alumni magazine for her work in successfully encouraging underrepresented students to pursue Computer Science and Cybersecurity. She received a bachelor's degree in Computer Science from Norfolk State University, a master's. degree in Computer Science from Johns Hopkins University and a doctoral degree from Pace University in New York.

*

Nancy Wilkins-Diehr directs the NSF-funded Science Gateways Community Institute and is a co-principal investigator on the NSF XSEDE award where she co-directs the Extended Collaborative Support program. She has been with the San Diego Supercomputer Center since 1993 and has held a variety of management positions there. Prior to that she held engineering positions with General Atomics and General Dynamics in San Diego. Nancy received her Bachelor's degree from Boston College in Mathematics and Philosophy and her Master's degree in Aerospace Engineering from San Diego State University.

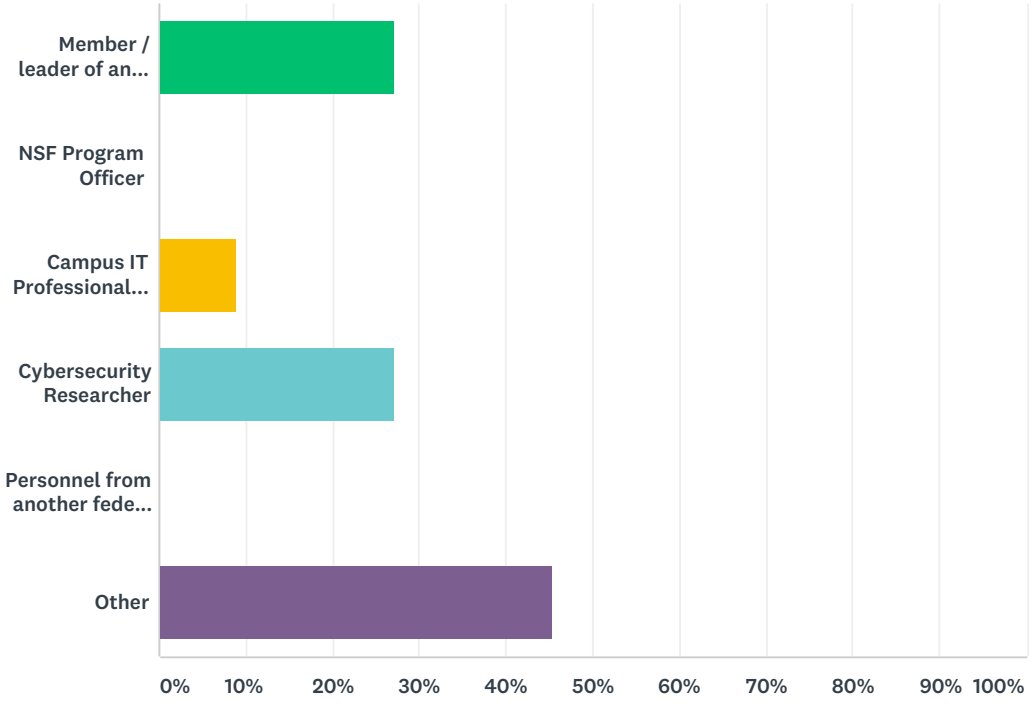
*

Alex Withers, Senior Security Engineer, NCSA.

Appendix H: Training Evaluation Summary Report and Attendee Survey Summary Report

Q1 Which options best describe your job or position? Check all that apply.

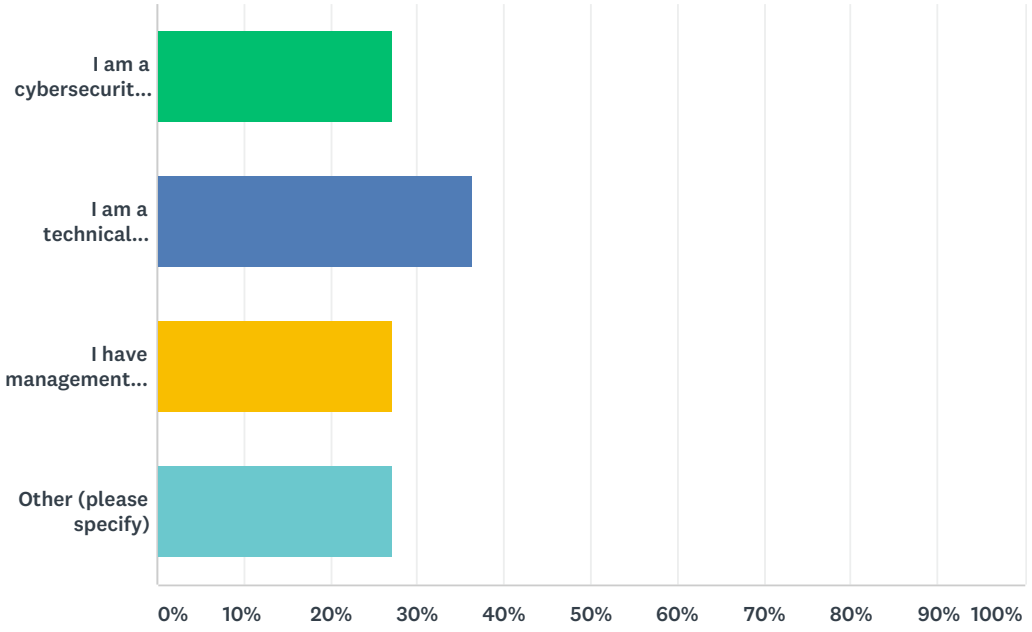
Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
Member / leader of an NSF project	27.27%	3
NSF Program Officer	0.00%	0
Campus IT Professional / CIO	9.09%	1
Cybersecurity Researcher	27.27%	3
Personnel from another federal program (NSA, DOE/ESNet, etc.)	0.00%	0
Other	45.45%	5
Total Respondents: 11		

Q2 How would you characterize your job in relationship to cybersecurity? Please check all that apply.

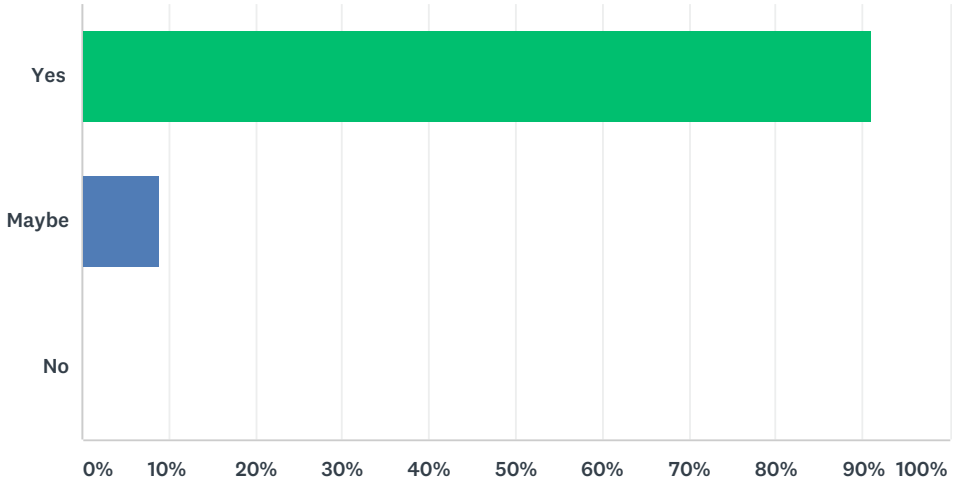
Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
I am a cybersecurity professional	27.27%	3
I am a technical professional who has knowledge of cybersecurity	36.36%	4
I have management responsibility for cybersecurity	27.27%	3
Other (please specify)	27.27%	3
Total Respondents: 11		

Q3 Based on your overall experience with the August 15 training sessions, would you participate in training offered at future summits?

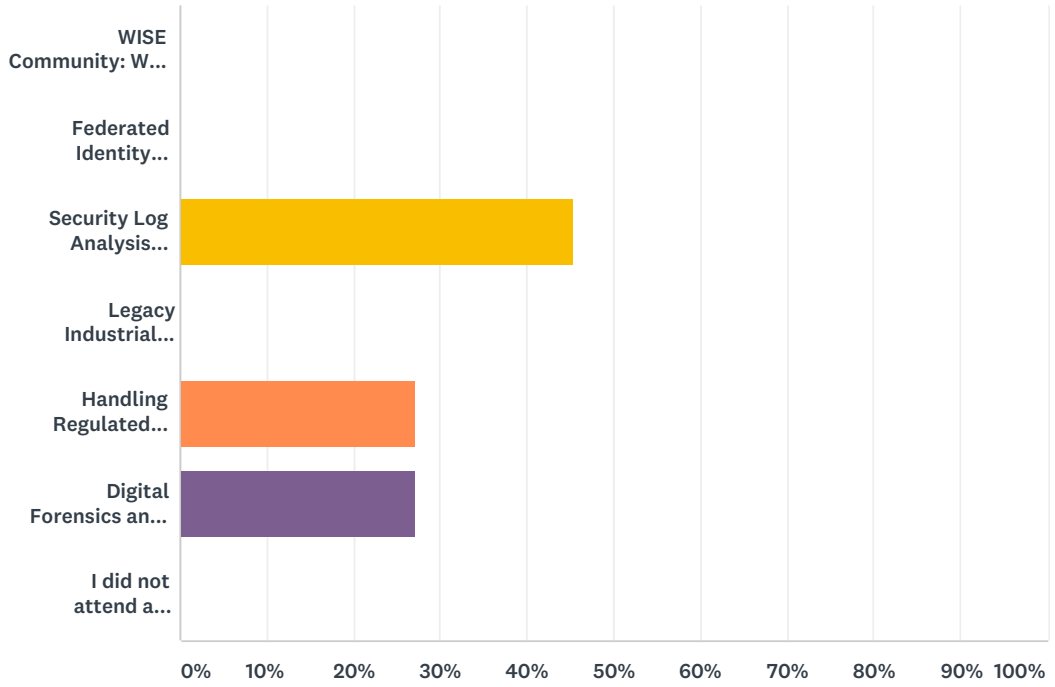
Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
Yes	90.91%	10
Maybe	9.09%	1
No	0.00%	0
TOTAL		11

Q5 Which morning session did you attend?

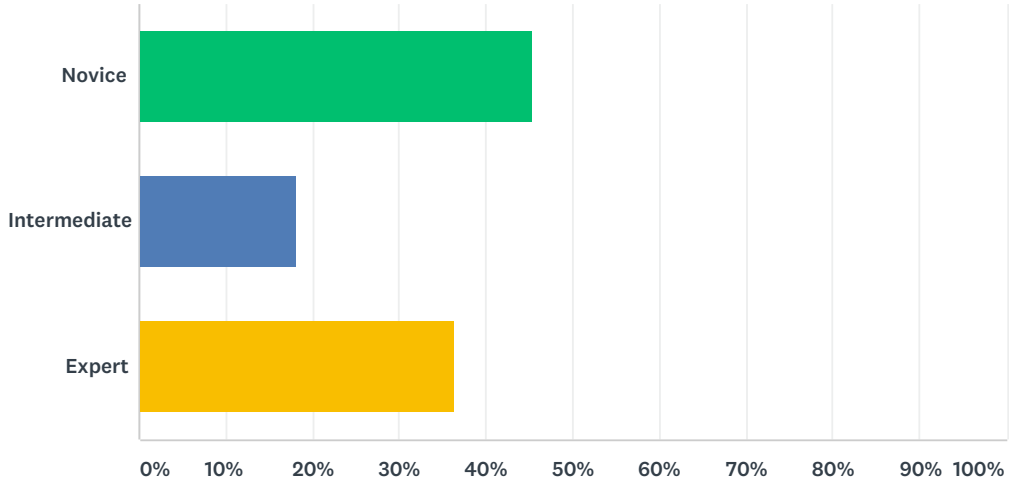
Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
WISE Community: WISE Information Security for Collaborating E-Infrastructures	0.00%	0
Federated Identity Management for Research Organizations	0.00%	0
Security Log Analysis Training	45.45%	5
Legacy Industrial Control Systems - Secure / Replace / Ignore?	0.00%	0
Handling Regulated Government Data, Protected Health Information, and CUI	27.27%	3
Digital Forensics and Incident Response	27.27%	3
I did not attend a morning session	0.00%	0
TOTAL		11

Q6 How would you rate your level of pre-training familiarity with the topics covered by this morning training session?

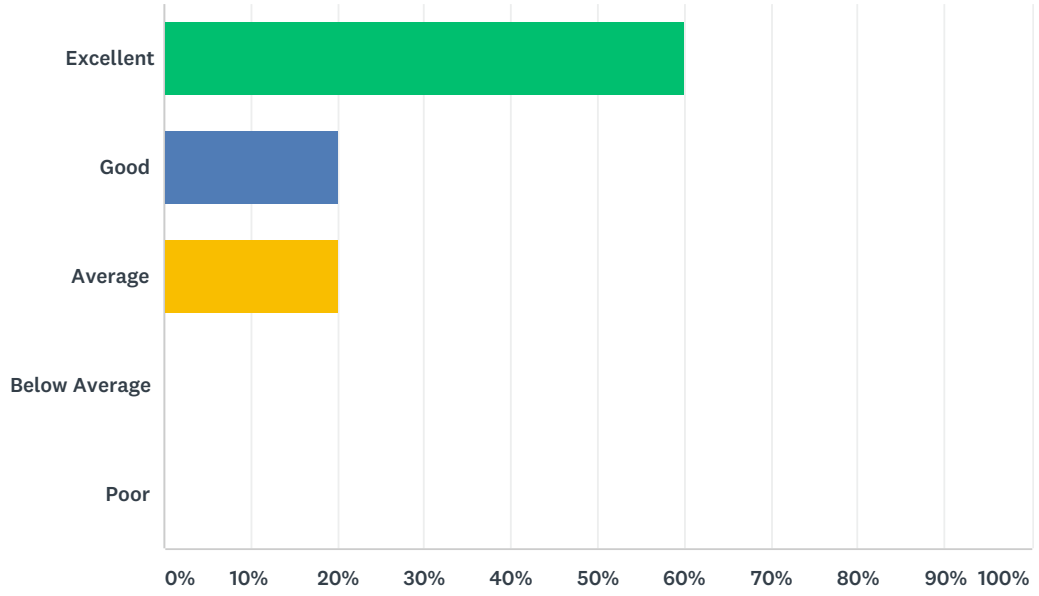
Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
Novice	45.45%	5
Intermediate	18.18%	2
Expert	36.36%	4
TOTAL		11

Q7 How would you rate your overall experience with the morning training?

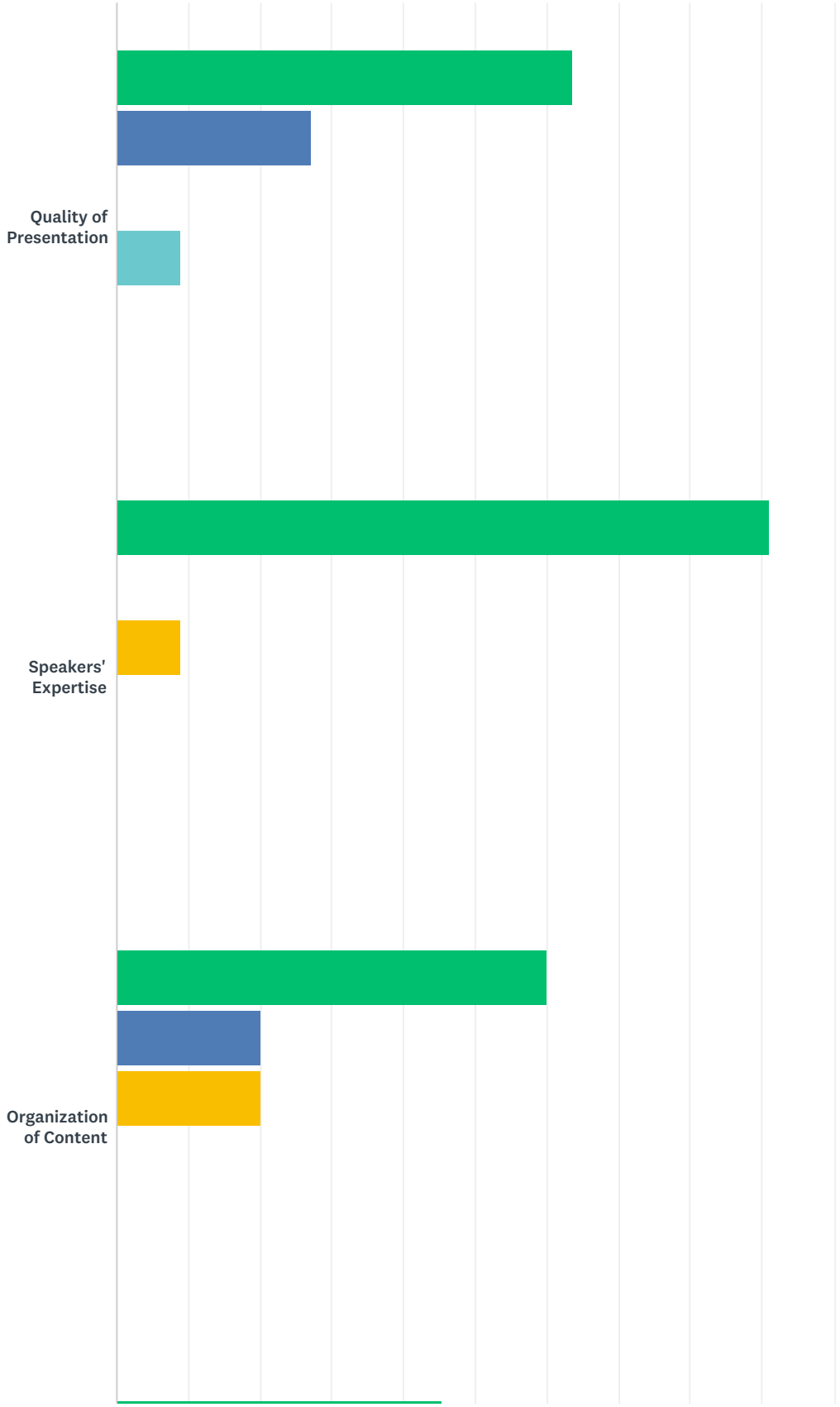
Answered: 10 Skipped: 1

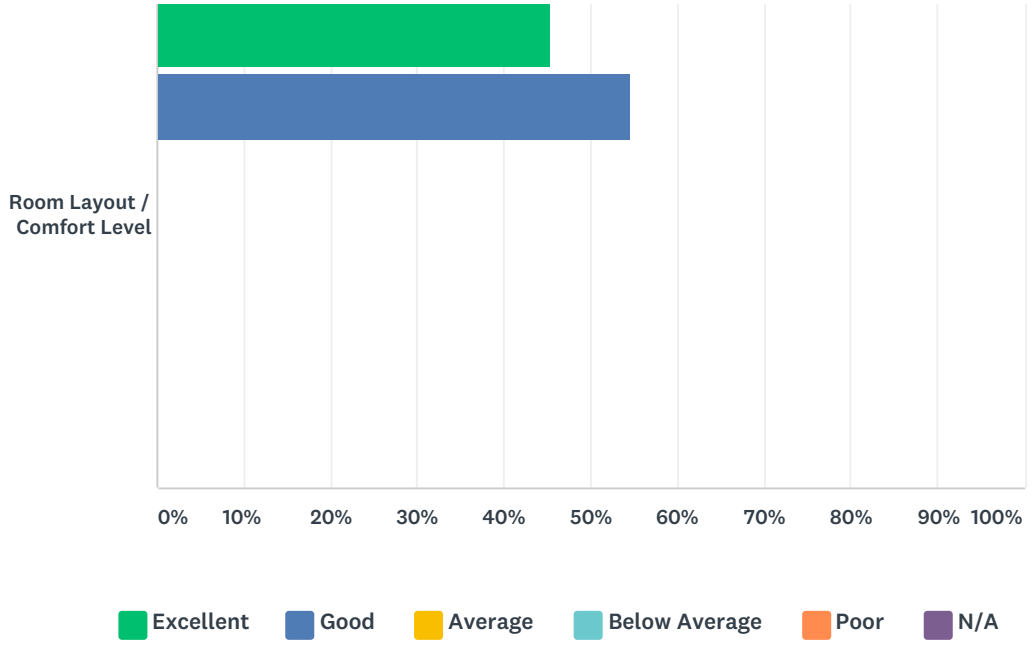


ANSWER CHOICES	RESPONSES	
Excellent	60.00%	6
Good	20.00%	2
Average	20.00%	2
Below Average	0.00%	0
Poor	0.00%	0
TOTAL		10

Q8 Please rate your experience with the morning training in these areas:

Answered: 11 Skipped: 0

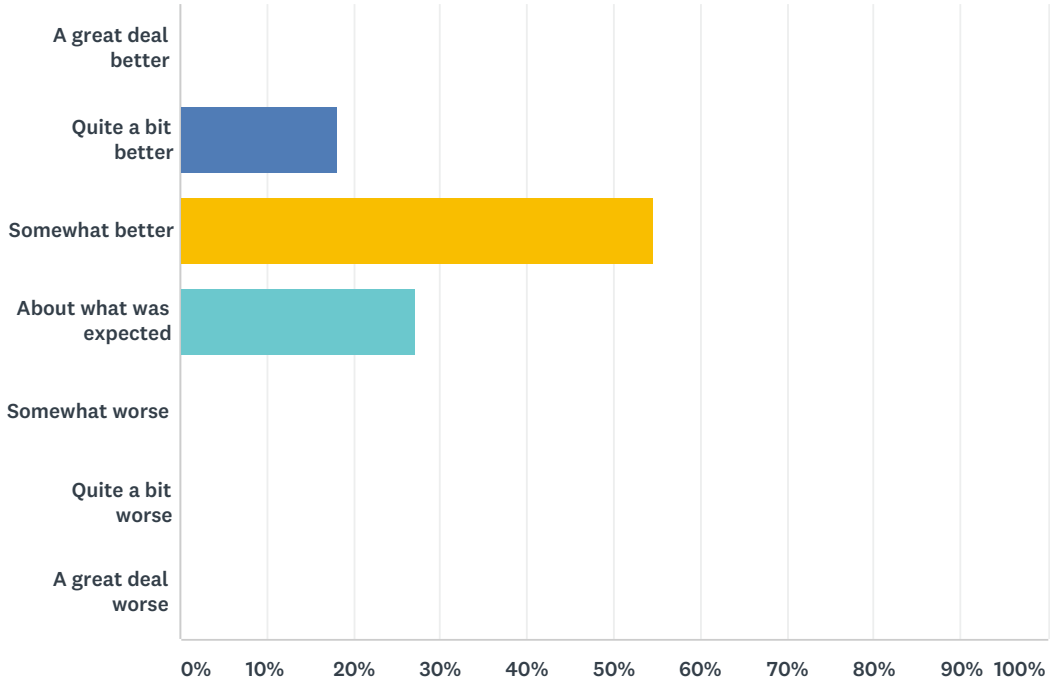




	EXCELLENT	GOOD	AVERAGE	BELOW AVERAGE	POOR	N/A	TOTAL RESPONDENTS
Quality of Presentation	63.64% 7	27.27% 3	0.00% 0	9.09% 1	0.00% 0	0.00% 0	11
Speakers' Expertise	90.91% 10	0.00% 0	9.09% 1	0.00% 0	0.00% 0	0.00% 0	11
Organization of Content	60.00% 6	20.00% 2	20.00% 2	0.00% 0	0.00% 0	0.00% 0	10
Room Layout / Comfort Level	45.45% 5	54.55% 6	0.00% 0	0.00% 0	0.00% 0	0.00% 0	11

Q9 Was this morning training better than what you expected, worse than what you expected, or about what you expected?

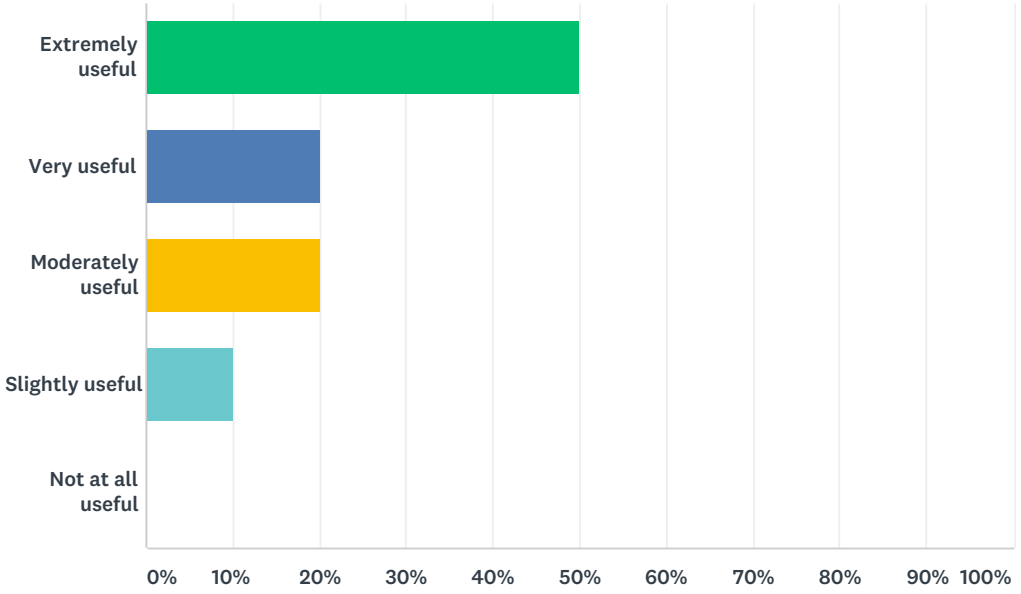
Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
A great deal better	0.00%	0
Quite a bit better	18.18%	2
Somewhat better	54.55%	6
About what was expected	27.27%	3
Somewhat worse	0.00%	0
Quite a bit worse	0.00%	0
A great deal worse	0.00%	0
TOTAL		11

Q10 How useful to your work was this morning training?

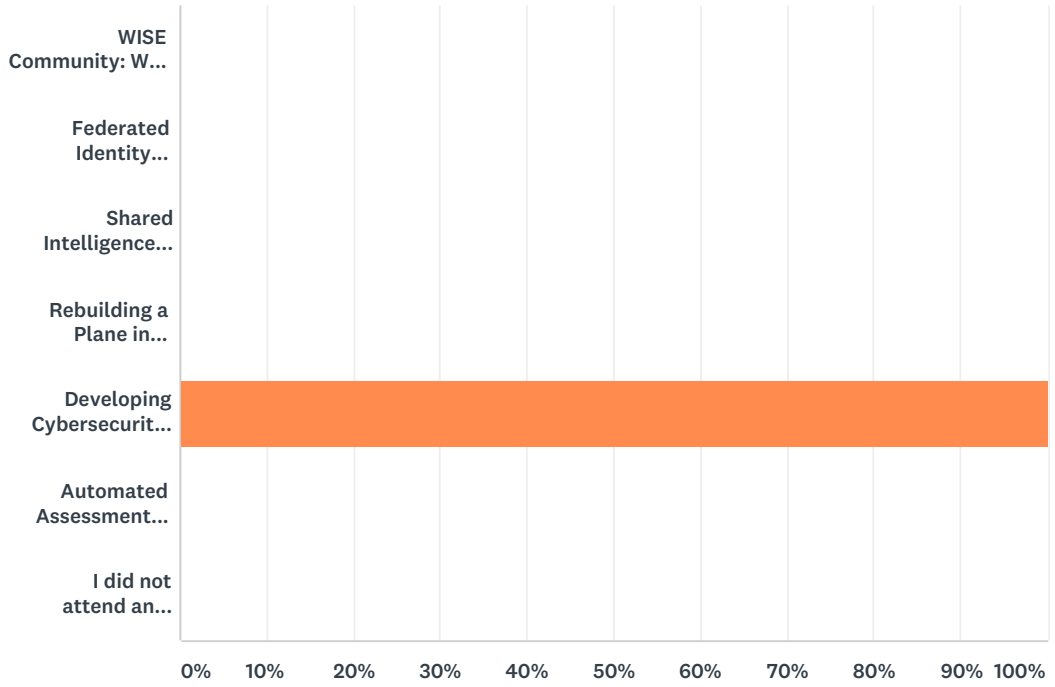
Answered: 10 Skipped: 1



ANSWER CHOICES	RESPONSES	
Extremely useful	50.00%	5
Very useful	20.00%	2
Moderately useful	20.00%	2
Slightly useful	10.00%	1
Not at all useful	0.00%	0
TOTAL		10

Q13 Which afternoon session did you attend?

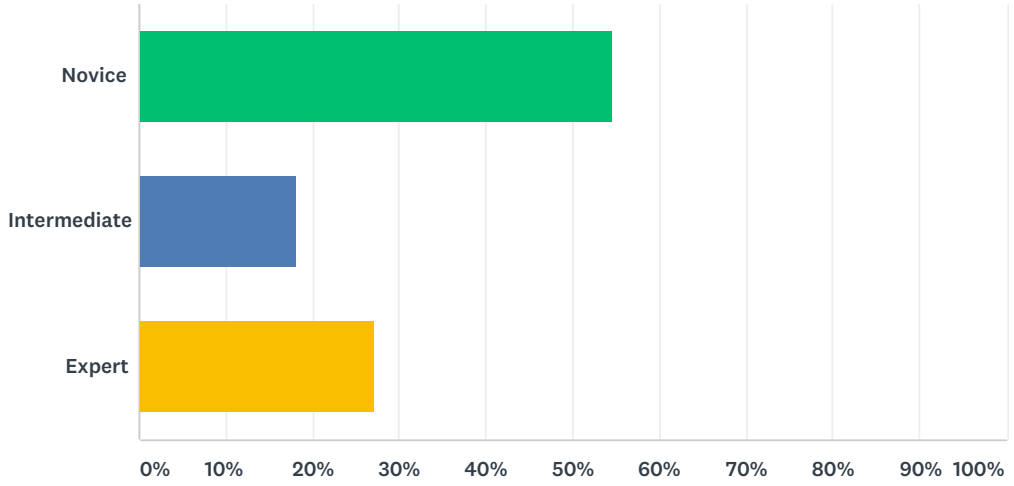
Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
WISE Community: WISE Information Security for Collaborating E-Infrastructures	0.00%	0
Federated Identity Management for Research Organizations	0.00%	0
Shared Intelligence Platform for Protecting our National Cyberinfrastructure	0.00%	0
Rebuilding a Plane in Flight: Refractors Under Pressure	0.00%	0
Developing Cybersecurity Programs for NSF Projects	100.00%	11
Automated Assessment Tools - Theory & Practice	0.00%	0
I did not attend an afternoon session.	0.00%	0
TOTAL		11

Q14 How would you rate your level of pre-training familiarity with the topics covered by this afternoon training session?

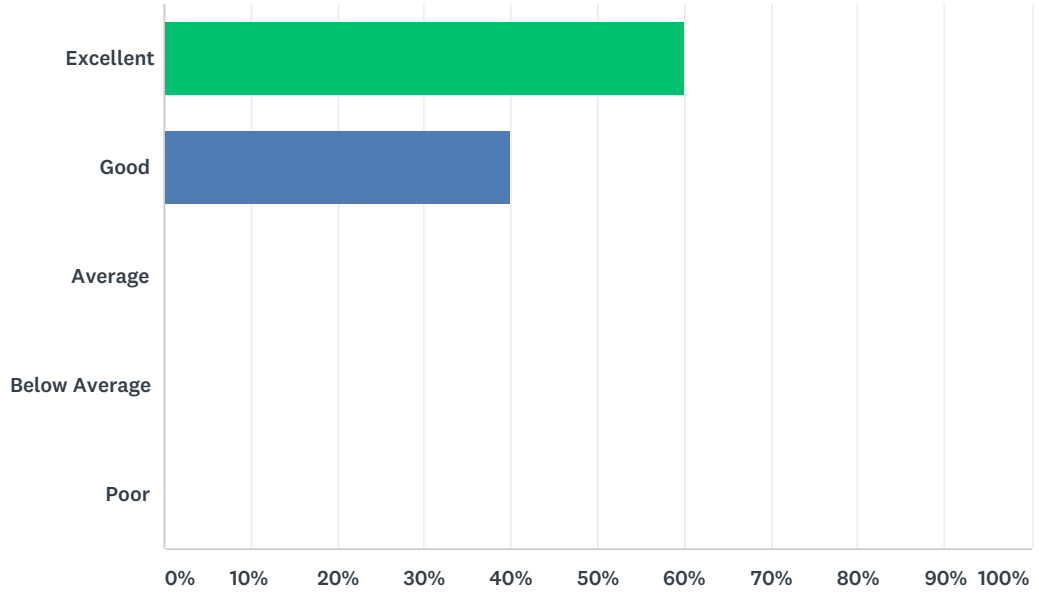
Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
Novice	54.55%	6
Intermediate	18.18%	2
Expert	27.27%	3
TOTAL		11

Q15 How would you rate your overall experience with the afternoon training?

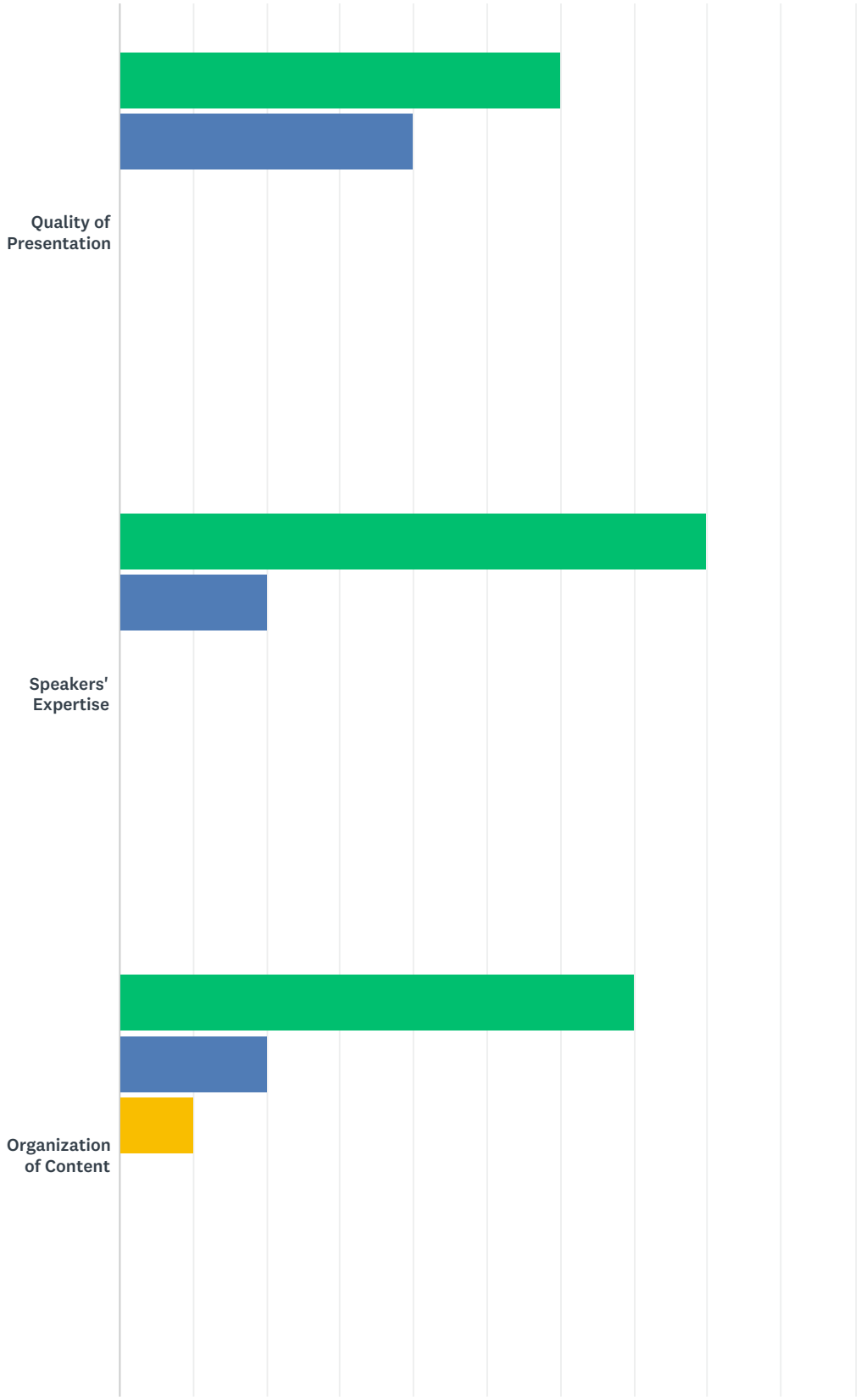
Answered: 10 Skipped: 1

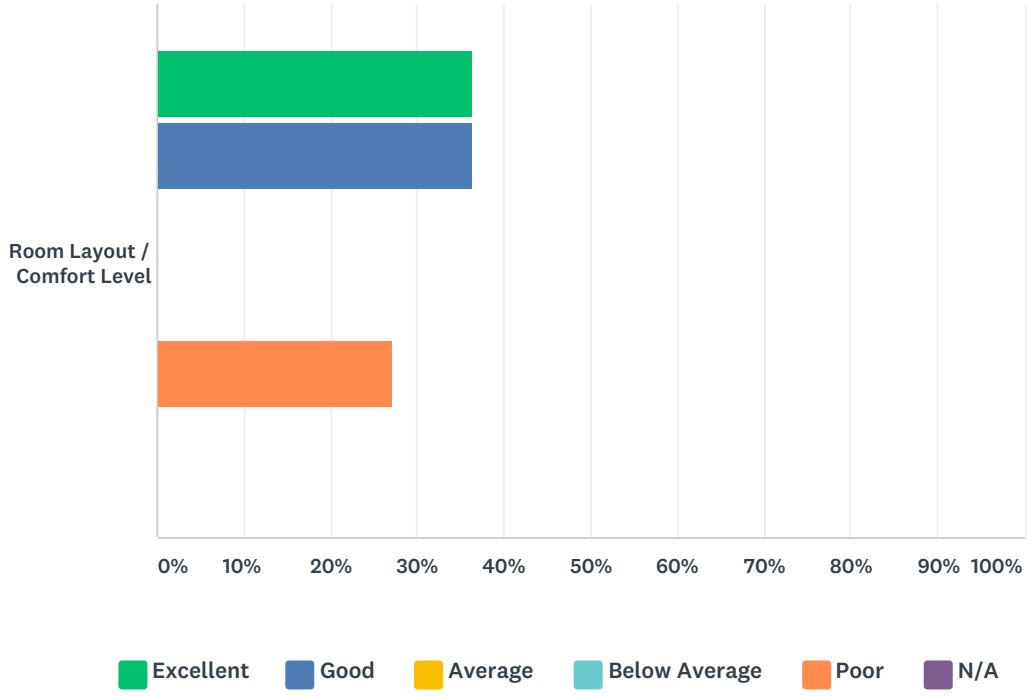


ANSWER CHOICES	RESPONSES	
Excellent	60.00%	6
Good	40.00%	4
Average	0.00%	0
Below Average	0.00%	0
Poor	0.00%	0
TOTAL		10

Q16 Please rate your experience with the afternoon training in these areas:

Answered: 11 Skipped: 0

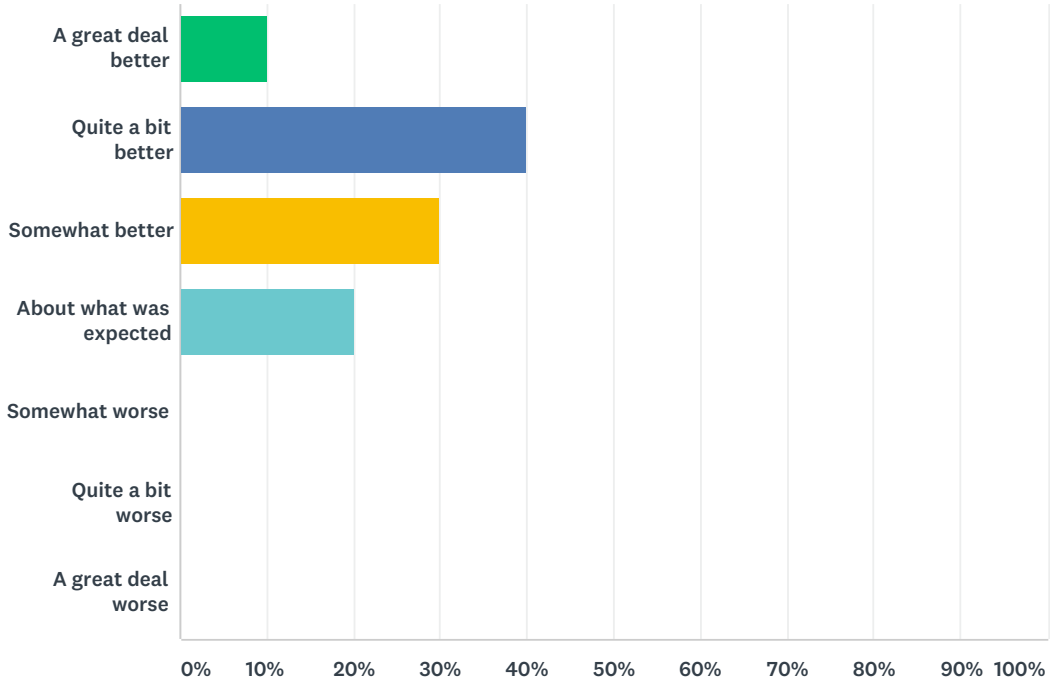




	EXCELLENT	GOOD	AVERAGE	BELOW AVERAGE	POOR	N/A	TOTAL RESPONDENTS
Quality of Presentation	60.00% 6	40.00% 4	0.00% 0	0.00% 0	0.00% 0	0.00% 0	10
Speakers' Expertise	80.00% 8	20.00% 2	0.00% 0	0.00% 0	0.00% 0	0.00% 0	10
Organization of Content	70.00% 7	20.00% 2	10.00% 1	0.00% 0	0.00% 0	0.00% 0	10
Room Layout / Comfort Level	36.36% 4	36.36% 4	0.00% 0	0.00% 0	27.27% 3	0.00% 0	11

Q17 Was this afternoon training session better than what you expected, worse than what you expected, or about what you expected?

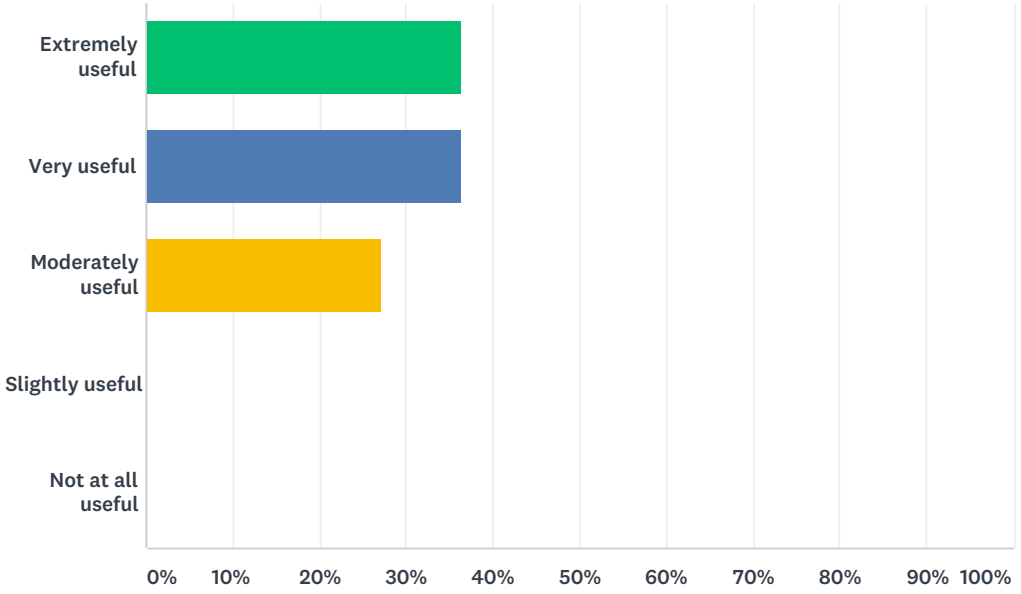
Answered: 10 Skipped: 1



ANSWER CHOICES	RESPONSES	
A great deal better	10.00%	1
Quite a bit better	40.00%	4
Somewhat better	30.00%	3
About what was expected	20.00%	2
Somewhat worse	0.00%	0
Quite a bit worse	0.00%	0
A great deal worse	0.00%	0
TOTAL		10

Q18 How useful to your work was this afternoon training?

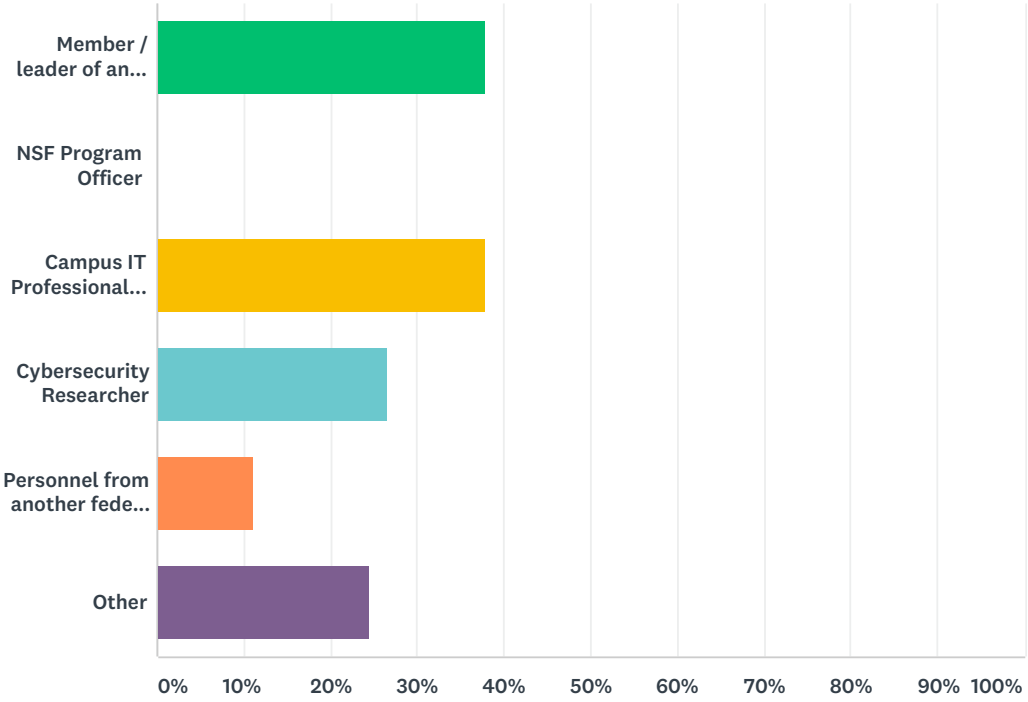
Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
Extremely useful	36.36%	4
Very useful	36.36%	4
Moderately useful	27.27%	3
Slightly useful	0.00%	0
Not at all useful	0.00%	0
TOTAL		11

Q1 Which options best describe your job or position? Check all that apply.

Answered: 45 Skipped: 0



ANSWER CHOICES	RESPONSES	
Member / leader of an NSF project	37.78%	17
NSF Program Officer	0.00%	0
Campus IT Professional / CIO	37.78%	17
Cybersecurity Researcher	26.67%	12
Personnel from another federal program (NSA, DOE/ESNet, etc.)	11.11%	5
Other	24.44%	11
Total Respondents: 45		

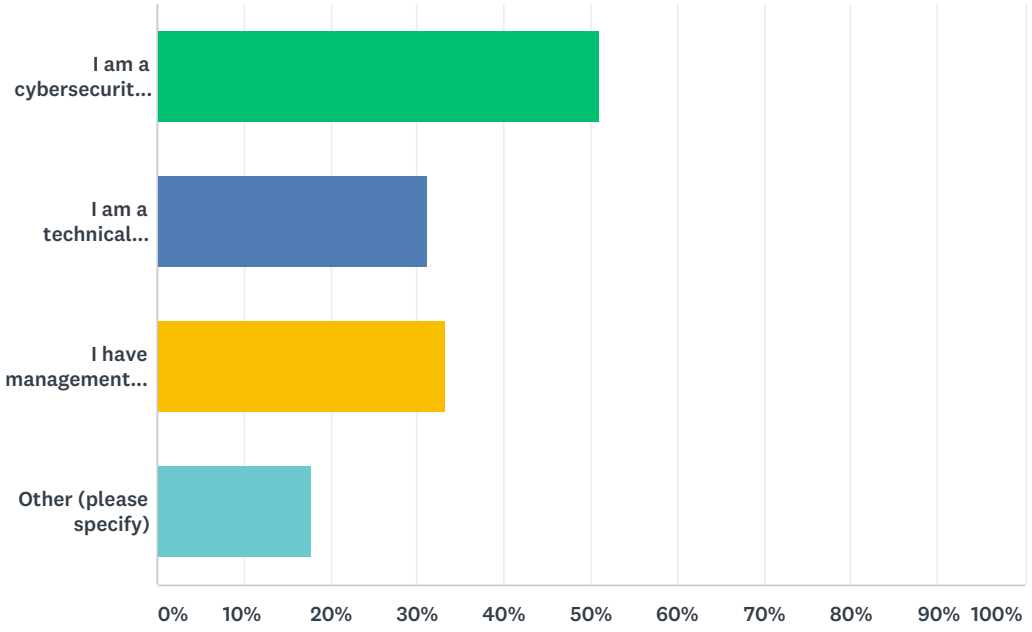
Q2 Where do you work primarily?

Answered: 45 Skipped: 0

ANSWER CHOICES	RESPONSES	
State/Province:	95.56%	43
Country:	100.00%	45

Q3 How would you characterize your job in relationship to cybersecurity? Please check all that apply.

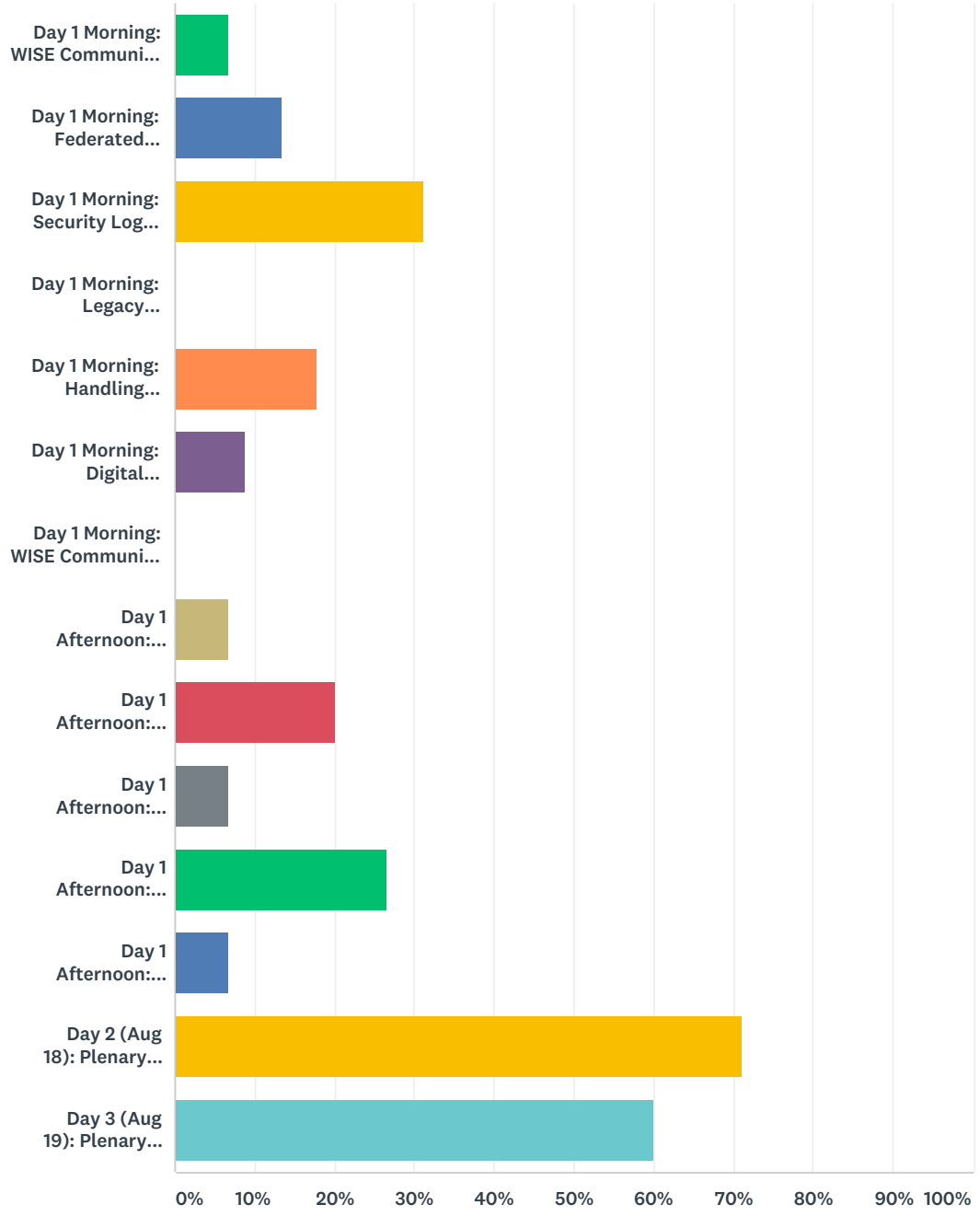
Answered: 45 Skipped: 0



ANSWER CHOICES	RESPONSES	
I am a cybersecurity professional	51.11%	23
I am a technical professional who has knowledge of cybersecurity	31.11%	14
I have management responsibility for cybersecurity	33.33%	15
Other (please specify)	17.78%	8
Total Respondents: 45		

Q4 What sessions of the summit did you attend? Check all that apply.

Answered: 45 Skipped: 0

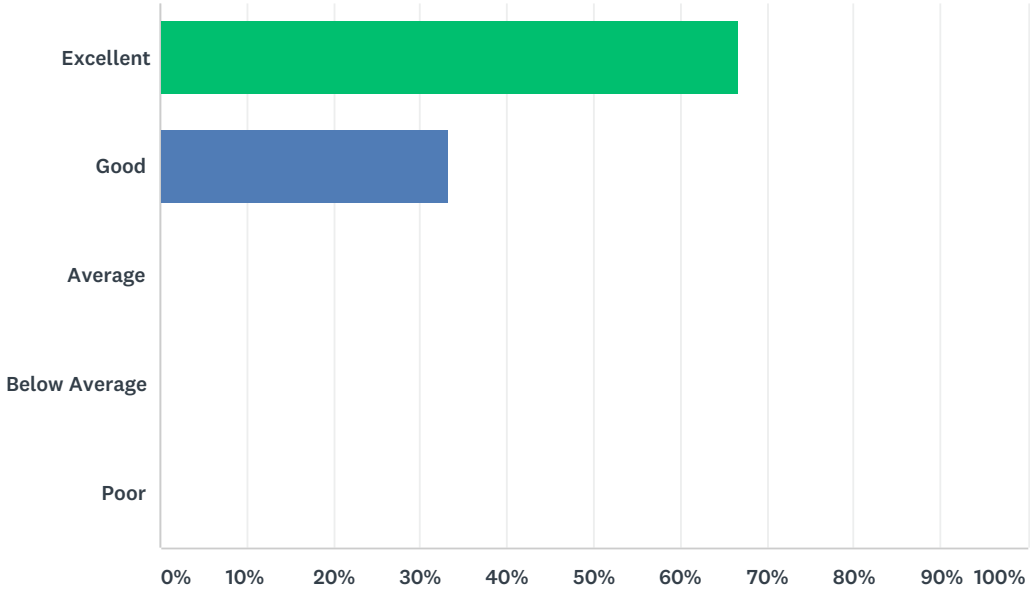


ANSWER CHOICES	RESPONSES	
Day 1 Morning: WISE Community: WISE Information Security for Collaborating E-Infrastructures	6.67%	3
Day 1 Morning: Federated Identity Management for Research Organizations	13.33%	6
Day 1 Morning: Security Log Analysis Training	31.11%	14
Day 1 Morning: Legacy Industrial Control Systems - Secure / Replace / Ignore?	0.00%	0
Day 1 Morning: Handling Regulated Government Data, Protected Health Information, and CUI	17.78%	8

Day 1 Morning: Digital Forensics and Incident Response	8.89%	4
Day 1 Morning: WISE Community: WISE Information Security for Collaborating E-Infrastructures (continued)	0.00%	0
Day 1 Afternoon: Federated Identity Management for Research Organizations (continued)	6.67%	3
Day 1 Afternoon: Shared Intelligence Platform for Protecting our National Cyberinfrastructure	20.00%	9
Day 1 Afternoon: Rebuilding a Plane in Flight: Refractors Under Pressure	6.67%	3
Day 1 Afternoon: Developing Cybersecurity Programs for NSF Projects	26.67%	12
Day 1 Afternoon: Automated Assessment Tools - Theory & Practice	6.67%	3
Day 2 (Aug 18): Plenary Session	71.11%	32
Day 3 (Aug 19): Plenary Session	60.00%	27
Total Respondents: 45		

Q5 How would you rate your overall experience with the 2017 summit?

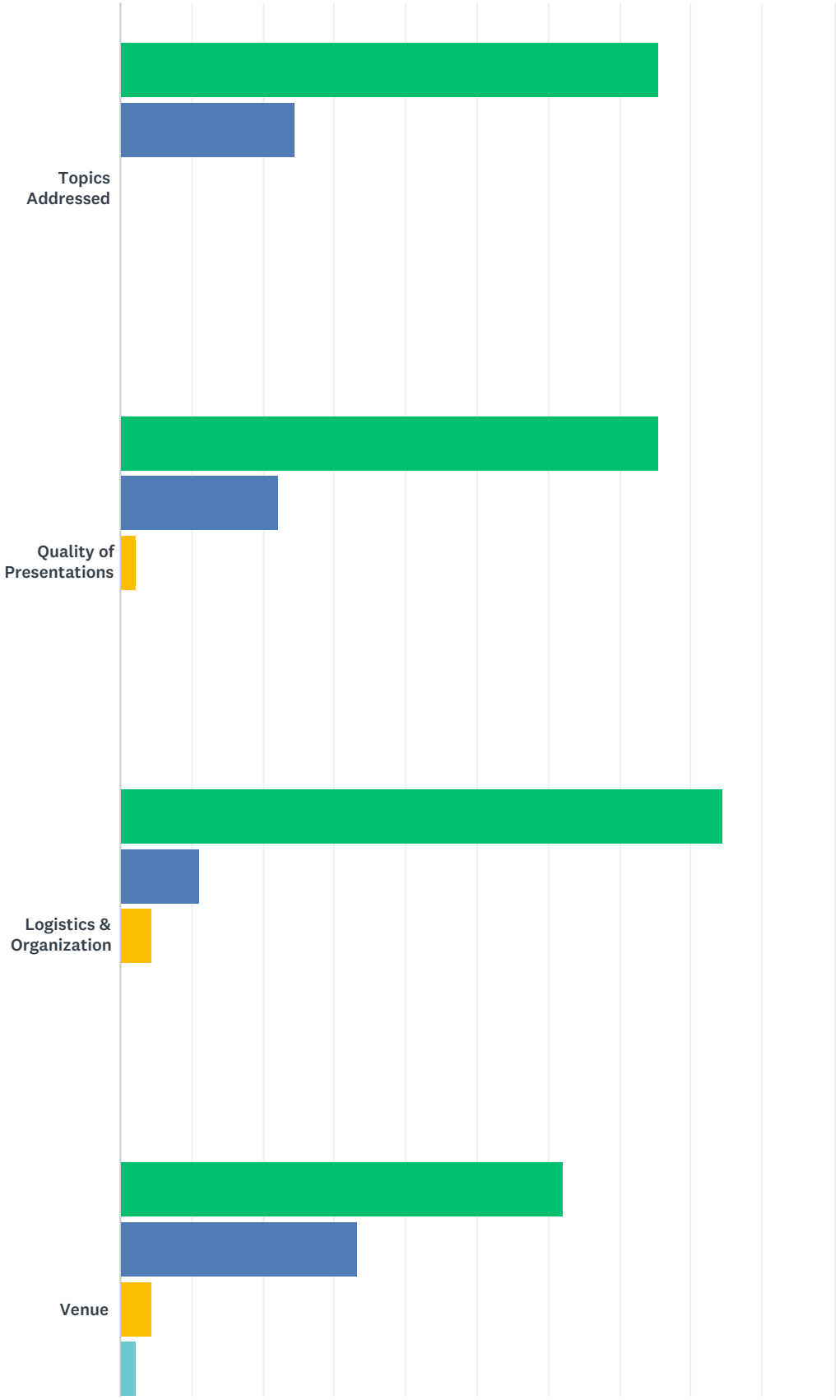
Answered: 45 Skipped: 0

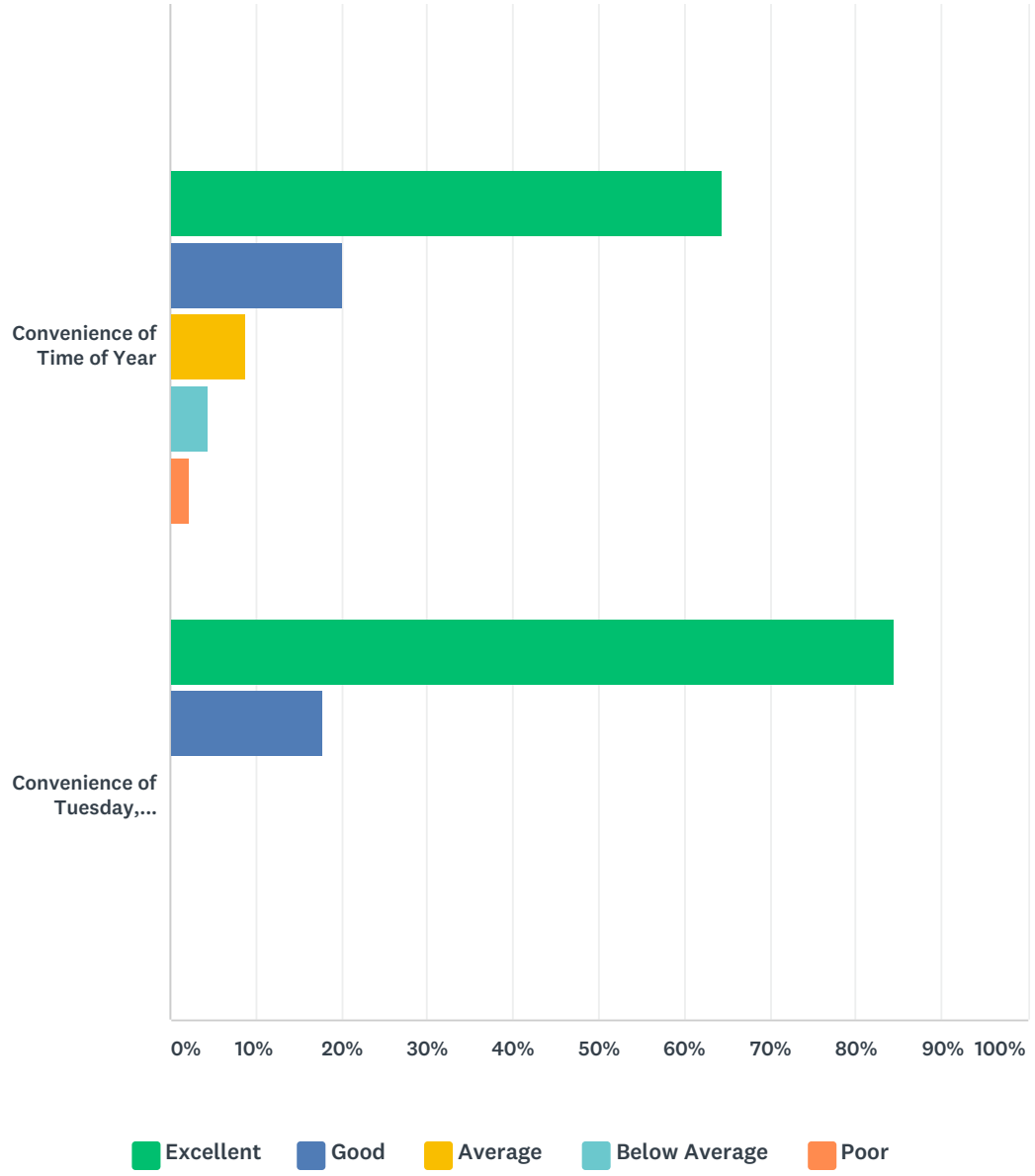


ANSWER CHOICES	RESPONSES	
Excellent	66.67%	30
Good	33.33%	15
Average	0.00%	0
Below Average	0.00%	0
Poor	0.00%	0
TOTAL		45

Q6 Please rate your experience with the 2017 summit in these areas:

Answered: 45 Skipped: 0

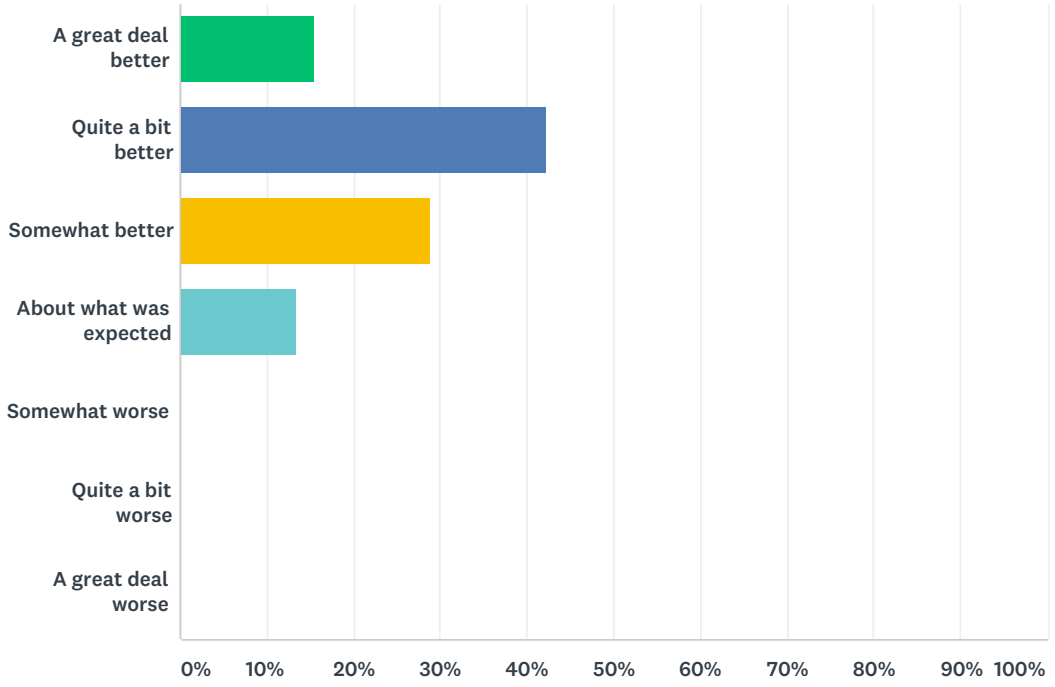




	EXCELLENT	GOOD	AVERAGE	BELOW AVERAGE	POOR	TOTAL RESPONDENTS
Topics Addressed	75.56% 34	24.44% 11	0.00% 0	0.00% 0	0.00% 0	45
Quality of Presentations	75.56% 34	22.22% 10	2.22% 1	0.00% 0	0.00% 0	45
Logistics & Organization	84.44% 38	11.11% 5	4.44% 2	0.00% 0	0.00% 0	45
Venue	62.22% 28	33.33% 15	4.44% 2	2.22% 1	0.00% 0	45
Convenience of Time of Year	64.44% 29	20.00% 9	8.89% 4	4.44% 2	2.22% 1	45
Convenience of Tuesday, Wednesday, Thursday Dates	84.44% 38	17.78% 8	0.00% 0	0.00% 0	0.00% 0	45

Q7 Was this summit better than what you expected, worse than what you expected, or about what you expected?

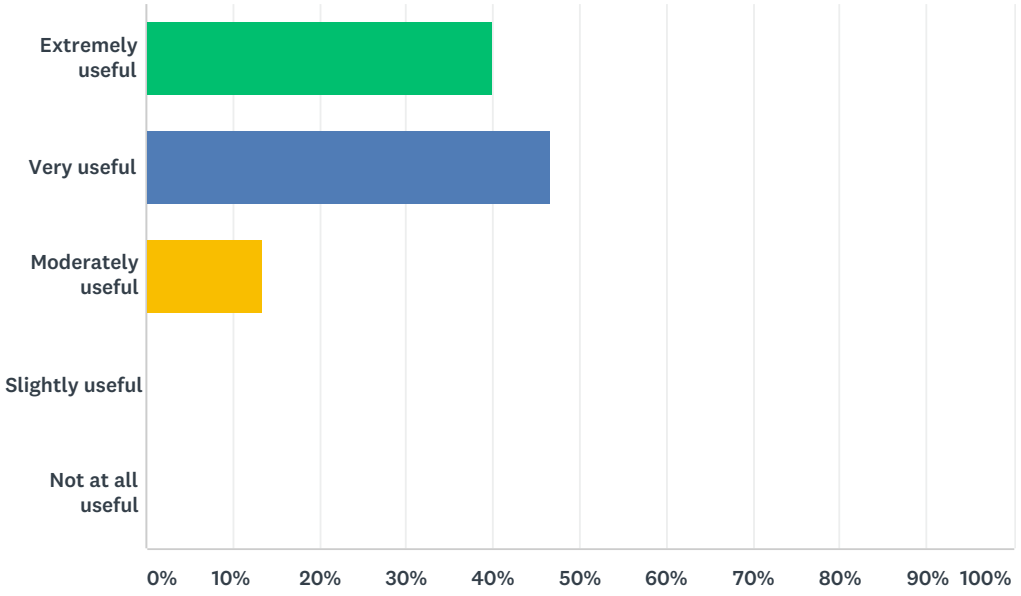
Answered: 45 Skipped: 0



ANSWER CHOICES	RESPONSES	
A great deal better	15.56%	7
Quite a bit better	42.22%	19
Somewhat better	28.89%	13
About what was expected	13.33%	6
Somewhat worse	0.00%	0
Quite a bit worse	0.00%	0
A great deal worse	0.00%	0
TOTAL		45

Q8 How useful to your work was the information discussed at the summit?

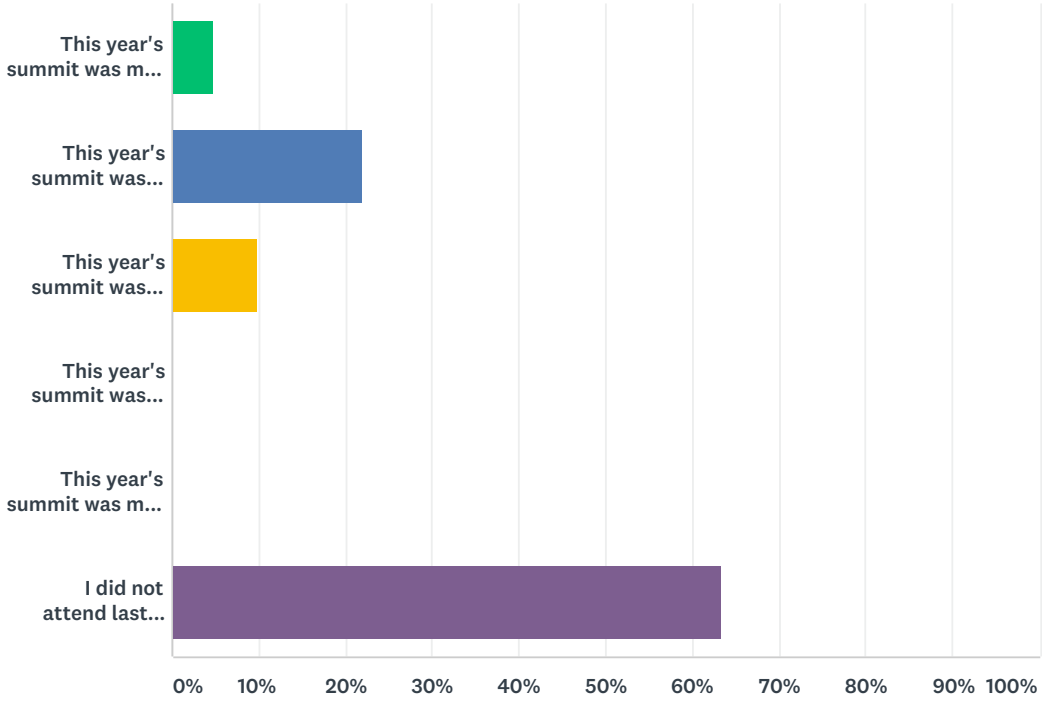
Answered: 45 Skipped: 0



ANSWER CHOICES	RESPONSES	
Extremely useful	40.00%	18
Very useful	46.67%	21
Moderately useful	13.33%	6
Slightly useful	0.00%	0
Not at all useful	0.00%	0
TOTAL		45

Q9 If you attended last year's summit, how does this year's compare?

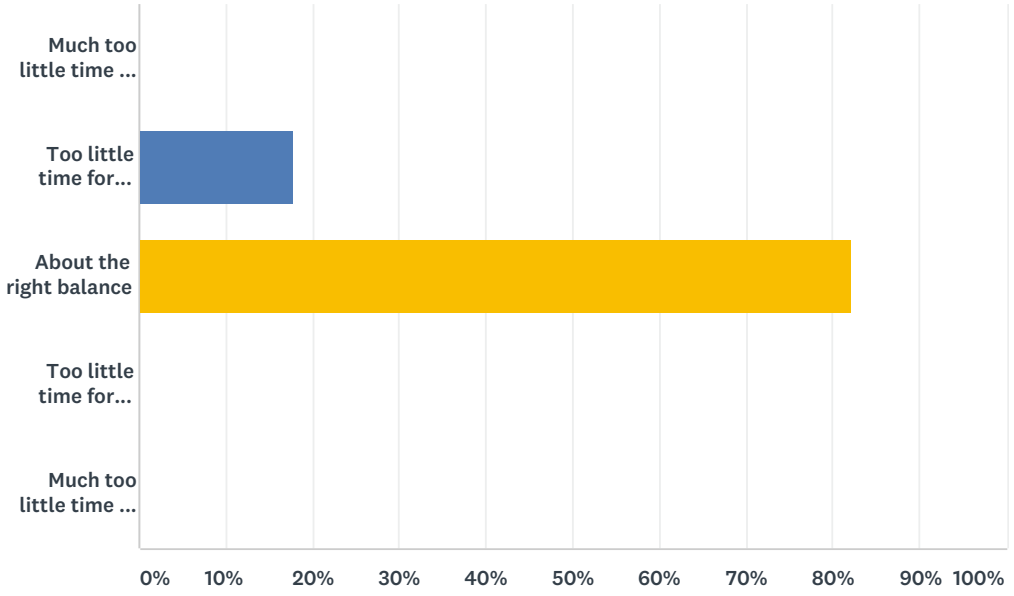
Answered: 41 Skipped: 4



ANSWER CHOICES	RESPONSES	
This year's summit was much better than last year's.	4.88%	2
This year's summit was better than last year's.	21.95%	9
This year's summit was about the same as last year's.	9.76%	4
This year's summit was worse than last year's.	0.00%	0
This year's summit was much worse than last year's.	0.00%	0
I did not attend last year's summit.	63.41%	26
TOTAL		41

Q10 How would you describe the balance between structured presentations and informal networking opportunities?

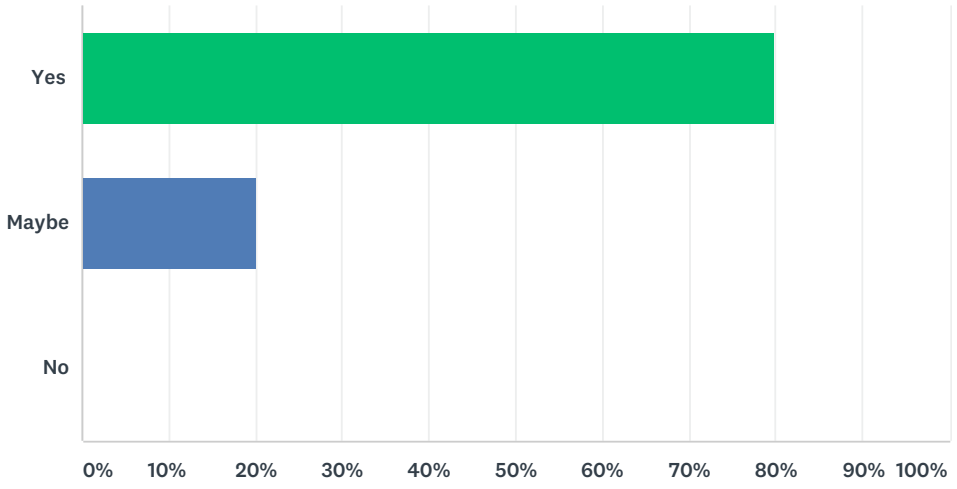
Answered: 45 Skipped: 0



ANSWER CHOICES	RESPONSES	
Much too little time for informal networking	0.00%	0
Too little time for informal networking	17.78%	8
About the right balance	82.22%	37
Too little time for structured presentations	0.00%	0
Much too little time for structured presentations	0.00%	0
TOTAL		45

Q11 Would you like to attend future summits?

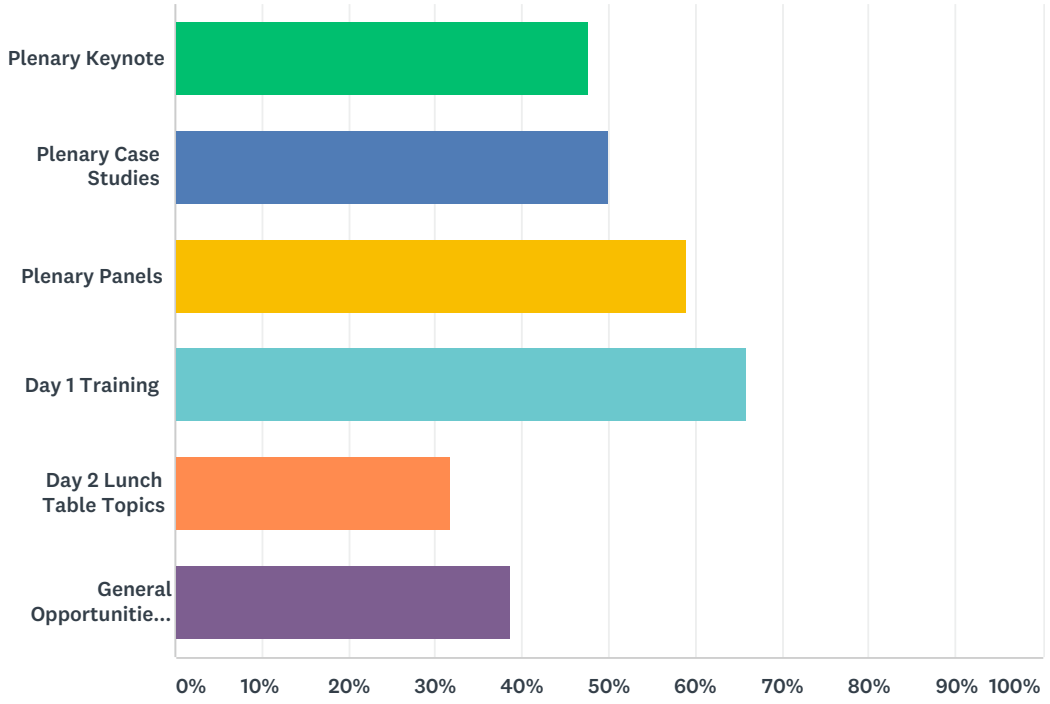
Answered: 45 Skipped: 0



ANSWER CHOICES	RESPONSES	
Yes	80.00%	36
Maybe	20.00%	9
No	0.00%	0
TOTAL		45

Q12 What presentation format(s) did you find most valuable? (You may select more than one.)

Answered: 44 Skipped: 1



ANSWER CHOICES	RESPONSES	
Plenary Keynote	47.73%	21
Plenary Case Studies	50.00%	22
Plenary Panels	59.09%	26
Day 1 Training	65.91%	29
Day 2 Lunch Table Topics	31.82%	14
General Opportunities to Network	38.64%	17
Total Respondents: 44		